Mario Linkies and Horst Karin

SAP® Security and Risk Management

Galileo Press
Bonn • Boston
# Contents at a Glance

## PART I  Basic Principles of Risk Management and IT Security  .......... 31

1 Risk and Control Management .............................................................. 33  
2 Enterprise Risk Management Strategy .................................................. 49  
3 Requirements ............................................................................................. 79  
4 Security Standards .................................................................................... 101  
5 IT Security ................................................................................................ 127  

## PART II  Security in SAP NetWeaver and Application Security .......... 153

6 Enterprise Risk Management (ERM) Navigation Control Map .......... 155  
7 Web Services, Enterprise Services, and Service-Oriented Architectures 175  
8 GRC Solutions in SAP BusinessObjects .................................................... 197  
9 SAP NetWeaver Application Server ............................................................. 257  
10 SAP NetWeaver Business Warehouse ...................................................... 309  
11 BI Solutions in SAP BusinessObjects ....................................................... 325  
12 SAP NetWeaver Process Integration .......................................................... 347  
13 SAP Partner Connectivity Kit .................................................................... 383  
14 Classic SAP Middleware ............................................................................... 391  
15 SAP NetWeaver Master Data Management .............................................. 423  
16 SAP NetWeaver Portal ............................................................................... 439  
17 SAP NetWeaver Mobile ............................................................................. 505  
18 SAP Auto-ID Infrastructure ....................................................................... 527  
19 SAP Solution Manager ............................................................................... 537  
20 Authorizations in SAP ERP ....................................................................... 555  
21 SAP ERP Human Capital Management and Data Protection .......... 599  
22 SAP Strategic Enterprise Management ..................................................... 619  
23 SAP Customer Relationship Management ............................................... 625  
24 SAP Supply Chain Management .............................................................. 639  
25 SAP Supplier Relationship Management ............................................... 647  
26 Industry-Specific SAP Solution Portfolios ............................................. 667  
27 Database Server ....................................................................................... 677  
28 User Interfaces .......................................................................................... 689
Contents

Preface by Wolfgang Lassmann ................................................................. 19
Preface by Monika Egle ............................................................................. 21
Preface by Jose Estrada ............................................................................. 23
Introduction .................................................................................................. 25

PART I Basic Principles of Risk Management and IT Security

1 Risk and Control Management ................................................................. 33

1.1 Security Objectives .................................................................................. 34
1.2 Company Assets ....................................................................................... 36
  1.2.1 Types of Company Assets .................................................................. 38
  1.2.2 Classification of Company Assets ....................................................... 39
1.3 Risks .......................................................................................................... 40
  1.3.1 Types of Risks .................................................................................... 41
  1.3.2 Classification of Risks ......................................................................... 44
1.4 Controls ..................................................................................................... 45
  1.4.1 Types of Controls ............................................................................... 45
  1.4.2 Classification of Controls ..................................................................... 46

2 Enterprise Risk Management Strategy .................................................... 49

2.1 Status Quo ................................................................................................. 51
2.2 Components ............................................................................................. 52
  2.2.1 General Framework ............................................................................. 56
  2.2.2 Strategy ............................................................................................... 57
  2.2.3 Methods ............................................................................................. 58
  2.2.4 Best Practices .................................................................................... 59
  2.2.5 Documentation ................................................................................... 59
2.3 Best Practices of an SAP Security Strategy .............................................. 60
  2.3.1 Procedure .......................................................................................... 60
  2.3.2 Principle of Information Ownership ..................................................... 68
  2.3.3 Identity Management .......................................................................... 74
## Contents

### 3 Requirements

#### 3.1 Legal Requirements

- **Sarbanes-Oxley Act (SOX)**
- **SOX Implementation in Japan**
- **Principles for IT-Supported Accounting Systems**
- **International Financial Reporting Standards**

#### 3.2 Industry-Specific Requirements

- **Food and Pharmaceutical Industry and Biomedical Engineering**
- **Finance and Banking Industry — Basel (I, II, III)**
- **Chemical Substances and Environmental Protection**

#### 3.3 Internal Requirements

### 4 Security Standards

#### 4.1 International Security Standards

- **ISO/IEC 27002:2005**
- **CobiT**
- **ITIL**
- **COSO**

#### 4.2 Country-Specific Security Standards

- **NIST Special Publication 800-12**
- **IT Baseline Protection Manual**
- **PIPEDA**

### 5 IT Security

#### 5.1 Cryptography

- **Symmetric Encryption Procedure**
- **Asymmetric Encryption Procedure**
- **Elliptic Curve Cryptography**
- **Hybrid Encryption Procedure**
- **SSL Encryption**
- **Hash Procedures**
- **Digital Signature**

#### 5.2 Public Key Infrastructure

#### 5.3 Authentication Procedures

- **User Name and Password**
- **Challenge Response**
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.3 Kerberos</td>
<td>141</td>
</tr>
<tr>
<td>5.3.4 Secure Token</td>
<td>142</td>
</tr>
<tr>
<td>5.3.5 Digital Certificate</td>
<td>143</td>
</tr>
<tr>
<td>5.3.6 Biometric Procedures</td>
<td>143</td>
</tr>
<tr>
<td>5.4 Basic Principles of Networks and Security Aspects</td>
<td>144</td>
</tr>
<tr>
<td>5.4.1 OSI Reference Model</td>
<td>144</td>
</tr>
<tr>
<td>5.4.2 Overview of Firewall Technologies</td>
<td>150</td>
</tr>
<tr>
<td><strong>PART II Security in SAP NetWeaver and Application Security</strong></td>
<td></td>
</tr>
<tr>
<td>6 Enterprise Risk Management (ERM) Navigation Control Map</td>
<td>155</td>
</tr>
<tr>
<td>6.1 SAP Applications</td>
<td>163</td>
</tr>
<tr>
<td>6.2 SAP NetWeaver Components</td>
<td>165</td>
</tr>
<tr>
<td>6.3 Security Technologies</td>
<td>167</td>
</tr>
<tr>
<td>6.3.1 Authorizations, Risk and Change Management, and Auditing</td>
<td>168</td>
</tr>
<tr>
<td>6.3.2 Identity Management</td>
<td>169</td>
</tr>
<tr>
<td>6.3.3 Secure Authentication and SSO</td>
<td>171</td>
</tr>
<tr>
<td>6.3.4 Technical Security</td>
<td>172</td>
</tr>
<tr>
<td>6.4 Influencing Factors</td>
<td>173</td>
</tr>
<tr>
<td><strong>7 Web Services, Enterprise Services, and Service-Oriented Architectures</strong></td>
<td>175</td>
</tr>
<tr>
<td>7.1 Introduction and Technical Principles</td>
<td>177</td>
</tr>
<tr>
<td>7.2 Security Criteria for Web Services</td>
<td>181</td>
</tr>
<tr>
<td>7.2.1 Security and Risk Management for Service-Oriented Architectures</td>
<td>186</td>
</tr>
<tr>
<td>7.2.2 SAP Enterprise Services</td>
<td>187</td>
</tr>
<tr>
<td>7.2.3 Security Guidelines for SAP Enterprise Services</td>
<td>190</td>
</tr>
<tr>
<td>7.3 Service-Oriented Architectures and Governance</td>
<td>193</td>
</tr>
<tr>
<td><strong>8 GRC Solutions in SAP BusinessObjects</strong></td>
<td>197</td>
</tr>
<tr>
<td>8.1 Introduction and Functions</td>
<td>197</td>
</tr>
<tr>
<td>8.1.1 Goals of the GRC Solutions in SAP BusinessObjects</td>
<td>198</td>
</tr>
<tr>
<td>8.1.2 Methods of the GRC Solutions in SAP BusinessObjects</td>
<td>199</td>
</tr>
<tr>
<td>8.1.3 Planning the Deployment of GRC Solutions in SAP BusinessObjects</td>
<td>200</td>
</tr>
</tbody>
</table>
8.1.4 Overview of the GRC Solutions in SAP BusinessObjects .......................................................... 201
8.2 SAP BusinessObjects RM ........................................................................................................... 205
  8.2.1 Main Components .................................................................................................................. 205
  8.2.2 Phases .................................................................................................................................... 206
  8.2.3 Responsibilities ...................................................................................................................... 212
  8.2.4 Reporting .............................................................................................................................. 214
8.3 SAP BusinessObjects Access Control ......................................................................................... 214
  8.3.1 General Requirements on the SAP Authorization System ......................................................... 214
  8.3.2 Main Components .................................................................................................................. 221
8.4 SAP BusinessObjects Process Control ......................................................................................... 229
  8.4.1 My Home .............................................................................................................................. 232
  8.4.2 Compliance Structure ............................................................................................................. 233
  8.4.3 Evaluation Setup ..................................................................................................................... 234
  8.4.4 Evaluation Results ................................................................................................................ 234
  8.4.5 Certification .......................................................................................................................... 235
  8.4.6 Report Center .................................................................................................................... 236
  8.4.7 User Access ........................................................................................................................ 238
8.5 SAP BusinessObjects Global Trade Services (GTS) .................................................................... 238
  8.5.1 Compliance Management ..................................................................................................... 241
  8.5.2 Customs Management ....................................................................................................... 243
  8.5.3 Risk Management ................................................................................................................ 245
  8.5.4 Electronic Compliance Reporting ...................................................................................... 247
  8.5.5 System Administration ......................................................................................................... 247
8.6 SAP Environment, Health, and Safety (EHS) Management ......................................................... 248
  8.6.1 Overview ............................................................................................................................ 248
  8.6.2 Chemical Safety .................................................................................................................. 250
  8.6.3 Environment, Health, and Safety .................................................................................... 252
     8.6.4 Compliance with Product-Related Environmental Specifications ...................................... 252
  8.6.5 Compliance and Emission Management ............................................................................ 253
8.7 SAP BusinessObjects Sustainability Performance Management .................................................. 255
9 SAP NetWeaver Application Server ................................................................................................ 257
  9.1 Introduction and Functions ....................................................................................................... 257
  9.2 Risks and Controls ..................................................................................................................... 260
  9.3 Application Security ................................................................................................................ 269
     9.3.1 Technical Authorization Concept for Administrators ........................................................ 269
     9.3.2 Authorization Concept for Java Applications ................................................................. 277
     9.3.3 Restricting Authorizations for RFC Calls ....................................................................... 283
9.4 Technical Security ................................................................. 287
  9.4.1 Introducing an SSO Authentication Mechanism ............... 287
  9.4.2 Connecting the SAP NetWeaver AS to a Central
         LDAP Directory ................................................................. 289
  9.4.3 Changing the Default Passwords for Default Users ......... 291
  9.4.4 Configuring Security on the SAP Gateway ..................... 291
  9.4.5 Restricting Operating System Access ......................... 293
  9.4.6 Configuring Important Security System Parameters ......... 294
  9.4.7 Configuring Encrypted Communication Connections
         (SSL and SNC) ................................................................. 296
  9.4.8 Restricting Superfluous Internet Services .................. 301
  9.4.9 Secure Network Architecture for Using the SAP
         NetWeaver AS with the Internet .................................. 303
  9.4.10 Introducing an Application-Level Gateway to Make
         Internet Applications Secure .................................... 304
  9.4.11 Introducing Hardening Measures on the Operating
         System Level ................................................................. 304
  9.4.12 Introducing a Quality Assurance Process for Software
         Development ................................................................. 305
  9.4.13 Security and Authorization Checks in Custom ABAP
         and Java Program Code ............................................... 307

10 SAP NetWeaver Business Warehouse ...................................... 309
  10.1 Introduction and Functions ............................................. 309
  10.2 Risks and Controls ......................................................... 310
  10.3 Application Security ........................................................ 313
         10.3.1 Authorizations ....................................................... 314
         10.3.2 Analysis Authorizations ....................................... 318
         10.3.3 Other Concepts ....................................................... 319
  10.4 Technical Security ............................................................. 323

11 BI Solutions in SAP BusinessObjects ....................................... 325
  11.1 Introduction and Functions ............................................. 326
  11.2 Risks and Controls .......................................................... 327
  11.3 Application Security .......................................................... 332
         11.3.1 Authorization Concept for SAP BusinessObjects ....... 332
         11.3.2 Application Examples for Authorization Concepts ....... 339
         11.3.3 Securing the Administration Access and the Guest User ... 342
11.3.4 Configuring Password Rules ............................................ 342
11.3.5 Application Authorizations ............................................. 343
11.4 Technical Security .............................................................. 344
  11.4.1 External Authentication and SSO ................................. 344
  11.4.2 Using the Audit Function ............................................. 345
  11.4.3 Network Communication via SSL and CORBA Services ... 346

12 SAP NetWeaver Process Integration ........................................ 347
  12.1 Introduction and Functions ......................................................... 348
  12.2 Risks and Controls ................................................................. 350
  12.3 Application Security .............................................................. 357
    12.3.1 Authorizations for Enterprise Services Builder ................. 357
    12.3.2 Passwords and Authorizations for Technical Service Users .............................................. 359
    12.3.3 Authorizations for Administrative Access to SAP NetWeaver PI ........................................ 360
  12.3.4 Password Rules for Administrators ................................... 361
  12.4 Technical Security .............................................................. 361
    12.4.1 Definition of Technical Service Users for Communication Channels at Runtime ................................. 362
    12.4.2 Setting Up Encryption for Communication Channels ...... 363
    12.4.3 Digital Signature for XML-Based Messages .................... 371
    12.4.4 Encryption of XML-Based Messages ............................. 376
    12.4.5 Network-Side Security for Integration Scenarios .......... 376
    12.4.6 Audit of the Enterprise Services Builder ......................... 377
    12.4.7 Securing the File Adapter at the Operating System Level .......................................................... 379
    12.4.8 Encrypting PI Communication Channels and Web Services ....................................................... 380
    12.4.9 Security for Web Services ............................................. 380

13 SAP Partner Connectivity Kit ................................................... 383
  13.1 Introduction and Functions ......................................................... 383
  13.2 Risks and Controls ................................................................. 384
  13.3 Application Security .............................................................. 388
  13.4 Technical Security .............................................................. 388
    13.4.1 Separate Technical Service User for Every Connected Partner System ............................................. 389
    13.4.2 Setting Up Encryption for Communication Channels ...... 389
## 13.4.3 Digital Signature for XML-Based Messages

389

## 13.4.4 Network-Side Security for Integration Scenarios

389

## 13.4.5 Audit of the Message Exchange

389

## 13.4.6 Securing the File Adapter at the Operating System Level

390

### 14 Classic SAP Middleware

391

#### 14.1 SAP Web Dispatcher

391

- **14.1.1 Introduction and Functions**: 392
- **14.1.2 Risks and Controls**: 392
- **14.1.3 Application Security**: 395
- **14.1.4 Technical Security**: 395

#### 14.2 SAProuter

403

- **14.2.1 Introduction and Functions**: 403
- **14.2.2 Risks and Controls**: 404
- **14.2.3 Application Security**: 405
- **14.2.4 Technical Security**: 405

#### 14.3 SAP Internet Transaction Server (ITS)

407

- **14.3.1 Introduction and Functions**: 408
- **14.3.2 Risks and Controls**: 410
- **14.3.3 Application Security**: 413
- **14.3.4 Technical Security**: 415

### 15 SAP NetWeaver Master Data Management

423

#### 15.1 Introduction and Functions

423

#### 15.2 Risks and Controls

424

#### 15.3 Application Security

429

- **15.3.1 Identity Management and Authorizations**: 429
- **15.3.2 Revision Security**: 436

#### 15.4 Technical Security

436

- **15.4.1 Communication Security**: 436
- **15.4.2 Important Additional Components**: 437

### 16 SAP NetWeaver Portal

439

#### 16.1 Introduction and Functions

439

- **16.1.1 Technical Architecture**: 441
- **16.1.2 Description of the UME**: 443

#### 16.2 Risks and Controls

447
## Contents

### 16.3 Application Security
- 16.3.1 Structure and Design of Portal Roles ........................................ 456
- 16.3.2 Authorizations for the UME ................................................. 463
- 16.3.3 Portal Security Zones .......................................................... 464
- 16.3.4 Authentication Check for iView Access ............................... 470
- 16.3.5 Standard Portal Roles and Delegated User
  Administration ........................................................................ 470
- 16.3.6 Synchronization of Portal Roles with ABAP Roles ............. 473
- 16.3.7 Change Management Process for New Portal Content ... 480

### 16.4 Technical Security
- 16.4.1 Connecting SAP NetWeaver Portal to a Central LDAP
  Directory or SAP System ........................................................ 481
- 16.4.2 Implementation of an SSO Mechanism Based on a
  One-Factor Authentication ....................................................... 484
- 16.4.3 Implementation of an SSO Mechanism Based on an
  Integrated Authentication ....................................................... 487
- 16.4.4 Implementation of an SSO Mechanism Based on a
  Person-Related Certificates .................................................... 489
- 16.4.5 Configuration for Anonymous Access ............................ 491
- 16.4.6 Secure Initial Configuration ............................................ 492
- 16.4.7 Secure Network Architecture ........................................... 493
- 16.4.8 Introducing an Application-Level Gateway to Make
  Portal Applications Secure ................................................... 496
- 16.4.9 Configuration of Encrypted Communication Channels ... 500
- 16.4.10 Implementation of a Virus Scan for Avoiding a
  Virus Infection ................................................................. 502

### 17 SAP NetWeaver Mobile
- 17.1 Introduction and Functions ................................................... 505
- 17.2 Risks and Controls ................................................................ 508
- 17.3 Application Security .............................................................. 515
  - 17.3.1 Authorization Concept for Mobile Applications .......... 515
  - 17.3.2 Authorization Concept for Administration ................. 518
  - 17.3.3 Restricting the Authorizations of the RFC User to
    Back-End Applications ...................................................... 519
- 17.4 Technical Security ................................................................ 520
  - 17.4.1 Setting Up Encrypted Communications Connections .... 520
  - 17.4.2 Securing the Synchronization Communication .......... 521
  - 17.4.3 Deactivating Unnecessary Services on the
    SAP NetWeaver Mobile Server ............................................ 523
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>17.4.4 Secure Network Architecture</td>
<td>523</td>
</tr>
<tr>
<td>17.4.5 Monitoring</td>
<td>524</td>
</tr>
<tr>
<td>17.4.6 Secure Program Code</td>
<td>525</td>
</tr>
<tr>
<td>18 SAP Auto-ID Infrastructure</td>
<td>527</td>
</tr>
<tr>
<td>18.1 Introduction and Functions</td>
<td>527</td>
</tr>
<tr>
<td>18.2 Risks and Controls</td>
<td>529</td>
</tr>
<tr>
<td>18.3 Application Security</td>
<td>533</td>
</tr>
<tr>
<td>18.3.1 Authorization Concept for SAP Auto-ID Infrastructure</td>
<td>533</td>
</tr>
<tr>
<td>18.3.2 Authorization Concept for Administration</td>
<td>533</td>
</tr>
<tr>
<td>18.3.3 Restricting the Authorizations of the RFC User to Back-End Applications</td>
<td>534</td>
</tr>
<tr>
<td>18.3.4 Authentication, Password Rules, and Security</td>
<td>534</td>
</tr>
<tr>
<td>18.4 Technical Security</td>
<td>535</td>
</tr>
<tr>
<td>18.4.1 Setting Up Encrypted Communication Connections</td>
<td>535</td>
</tr>
<tr>
<td>18.4.2 Deactivating Unnecessary Services on the Server</td>
<td>535</td>
</tr>
<tr>
<td>18.4.3 Secure Network Architecture</td>
<td>535</td>
</tr>
<tr>
<td>19 SAP Solution Manager</td>
<td>537</td>
</tr>
<tr>
<td>19.1 Introduction and Functions</td>
<td>537</td>
</tr>
<tr>
<td>19.2 Risks and Controls</td>
<td>540</td>
</tr>
<tr>
<td>19.3 Application Security</td>
<td>544</td>
</tr>
<tr>
<td>19.4 Technical Security</td>
<td>550</td>
</tr>
<tr>
<td>19.4.1 Security Measures for User Access</td>
<td>550</td>
</tr>
<tr>
<td>19.4.2 System Monitoring Function</td>
<td>551</td>
</tr>
<tr>
<td>19.4.3 RFC Communication Security</td>
<td>551</td>
</tr>
<tr>
<td>19.4.4 Data Communication Security</td>
<td>552</td>
</tr>
<tr>
<td>19.4.5 Important Components of SAP NetWeaver</td>
<td>553</td>
</tr>
<tr>
<td>20 Authorizations in SAP ERP</td>
<td>555</td>
</tr>
<tr>
<td>20.1 Introduction and Functions</td>
<td>555</td>
</tr>
<tr>
<td>20.2 Risks and Controls</td>
<td>556</td>
</tr>
<tr>
<td>20.3 Application Security</td>
<td>563</td>
</tr>
<tr>
<td>20.3.1 Authentication</td>
<td>563</td>
</tr>
<tr>
<td>20.3.2 Authorizations</td>
<td>563</td>
</tr>
<tr>
<td>20.3.3 Other Authorization Concepts</td>
<td>578</td>
</tr>
<tr>
<td>20.3.4 Best-Practice Solutions</td>
<td>589</td>
</tr>
<tr>
<td>20.4 Technical Security</td>
<td>597</td>
</tr>
</tbody>
</table>
Contents

21 SAP ERP Human Capital Management and Data Protection ............................................ 599

21.1 Introduction and Functions .................................................................................. 599
  21.1.1 Data Protection in Human Resources ......................................................... 599
  21.1.2 Technical and Organizational Measures .................................................... 600
21.2 Risks and Controls .............................................................................................. 602
21.3 Application Security ............................................................................................ 609
  21.3.1 HR Master Data Authorizations ................................................................. 610
  21.3.2 Applicant Authorizations ............................................................................ 612
  21.3.3 Personnel Planning Authorizations ............................................................... 613
  21.3.4 Reporting Authorizations ........................................................................... 613
  21.3.5 Structural Authorizations .......................................................................... 613
  21.3.6 Authorizations for Personnel Development .............................................. 614
  21.3.7 Tolerance Periods for Authorizations .......................................................... 614
  21.3.8 Authorizations for Inspection Procedures ................................................. 614
  21.3.9 Customized Authorization Checks ............................................................... 614
  21.3.10 Indirect Role Assignment through the Organizational Structure ................... 615
  21.3.11 Additional Transactions Relevant to Internal Controls ............................... 615
21.4 Technical Security ............................................................................................... 617

22 SAP Strategic Enterprise Management .................................................................... 619

22.1 Introduction and Functions .................................................................................. 619
22.2 Risks and Controls .............................................................................................. 620
22.3 Application Security ............................................................................................ 622
22.4 Technical Security ............................................................................................... 623

23 SAP Customer Relationship Management ............................................................ 625

23.1 Introduction and Functions .................................................................................. 625
23.2 Risks and Controls .............................................................................................. 626
23.3 Application Security ............................................................................................ 628
  23.3.1 Authorizations in SAP CRM ....................................................................... 629
  23.3.2 Authorizations for Portal Roles ................................................................. 635
23.4 Technical Security ............................................................................................... 636
  23.4.1 Technical Protection of the Mobile Application ........................................... 636
  23.4.2 Important Additional Components ............................................................... 636
24 SAP Supply Chain Management ....................................................... 639
  24.1 Introduction and Functions ....................................................... 639
  24.2 Risks and Controls ................................................................. 640
  24.3 Application Security ............................................................... 641
    24.3.1 Authorizations for the Integrated Product and Process
      Engineering (IPPE) Workbench ........................................... 642
    24.3.2 Authorizations for Supply Chain Planning ....................... 642
    24.3.3 Authorizations for SAP Event Management .................... 643
  24.4 Technical Security ................................................................. 644
25 SAP Supplier Relationship Management ........................................ 647
  25.1 Introduction and Functions ....................................................... 647
  25.2 Risks and Controls ................................................................. 649
  25.3 Application Security ............................................................... 651
    25.3.1 Important Authorizations ............................................ 651
    25.3.2 Rules-Based Security Checks Using Business Partner
      Attributes ..................................................................... 659
    25.3.3 User Management ....................................................... 663
  25.4 Technical Security ................................................................. 664
    25.4.1 Security Environment Based on SAP NetWeaver ............. 664
    25.4.2 Security Environment for RFC Communication ............... 665
26 Industry-Specific SAP Solution Portfolios ..................................... 667
  26.1 Introduction and Functions ....................................................... 668
  26.2 Risks and Controls ................................................................. 668
  26.3 Application Security ............................................................... 671
    26.3.1 SAP MaxSecure Support .............................................. 671
    26.3.2 SAP Role Manager ...................................................... 672
  26.4 Technical Security ................................................................. 675
27 Database Server ........................................................................... 677
  27.1 Introduction and Functions ....................................................... 677
  27.2 Risks and Controls ................................................................. 678
  27.3 Application Security ............................................................... 681
  27.4 Technical Security ................................................................. 683
    27.4.1 Changing Default Passwords ....................................... 683
# Contents

27.4.2 Removing Unnecessary Database Users .......................... 686  
27.4.3 Limiting Database Access ............................................... 686  
27.4.4 Creation and Implementation of a Database Backup Concept ................................................................. 686  
27.4.5 Filtering Database Queries ............................................. 687  
27.4.6 Creation and Implementation of an Upgrade Concept .... 688  

## 28 User Interfaces ........................................................................... 689  

28.1 SAP GUI ..................................................................................... 689  
28.1.1 Introduction and Functions ............................................ 689  
28.1.2 Risks and Controls .......................................................... 690  
28.1.3 Application Security ....................................................... 693  
28.1.4 Technical Security ........................................................... 698  

28.2 Web Browser .............................................................................. 701  
28.2.1 Introduction and Functions ............................................ 702  
28.2.2 Risks and Controls .......................................................... 702  
28.2.3 Application Security ....................................................... 704  
28.2.4 Technical Security ........................................................... 704  

28.3 Mobile Devices ........................................................................... 706  
28.3.1 Introduction and Functions ............................................ 706  
28.3.2 Risks and Controls .......................................................... 707  
28.3.3 Application Security ....................................................... 712  
28.3.4 Technical Security ........................................................... 712  

## Appendices ..................................................................................... 717  

A Bibliography ......................................................................................... 717  
B The Authors ......................................................................................... 719  

Index ......................................................................................................... 721
Data exchange between internal systems and external applications of business partners, customers, and organizations is an essential process in all system architectures. SAP NetWeaver Process Integration (PI) helps you reduce the number of direct interfaces between SAP and non-SAP applications. Where data is exchanged, however, security aspects assume a critical role; these are explained in this chapter.

12 SAP NetWeaver Process Integration

With SAP NetWeaver PI, SAP provides an enhanced integration platform for processes within distributed business applications. The objective is to integrate both SAP and non-SAP applications via a central platform using flexible web services or via interfaces. Thus, the number of required direct interfaces between individual applications can be reduced considerably. So SAP NetWeaver PI increasingly assumes the role of a powerful SAP middleware that not only enables integration using traditional interfaces but also lays the foundation for service-oriented architectures (SOAs) (see Chapter 7, Web Services, Enterprise Services, and Service-Oriented Architectures) and thus for process integration within and between companies based on an Enterprise Service Bus (ESB).

SAP NetWeaver PI relies on existing standards like web services (Simple Object Access Protocol (SOAP)), Remote Function Call (RFC), File Transfer Protocol (FTP), and other available protocols. It can also use interfaces (called connectors in the PI context) to Enterprise Application Integration (EAI) standards like RosettaNet or the chemical integration standard, Chemistry Industry Data eXchange (CIDX). SAP NetWeaver PI is predestinated for deployment in service-oriented architectures: The current release, Release 7.1, contains the Enterprise Services Repository, which serves as a structured directory for enterprise services.

Because SAP NetWeaver PI can run on both the ABAP stack and the Java stack of SAP NetWeaver Application Server (AS) (AS ABAP usage type, AS Java usage type, JEE5 for SAP NetWeaver PI), the security of “traditional” PI functions from Release 3.0 (SAP Exchange Infrastructure (XI)) and security characteristics and risks of new functions must be considered.
12.1 Introduction and Functions

SAP NetWeaver PI supports three communication variants, two of which are controlled directly by the PI architecture and its components:

- **Communication via the PI Integration Server**
  The PI Integration Server controls the forwarding of a message or web service integration between sender and recipient or provider and consumer. The communication partners are determined statically or dynamically using the mapping or routing functions of the integration server.

- **Communication using the PI Advanced Adapter Engine**
  If communication is supposed to be performed via the PI Advanced Adapter Engine, sender, recipient, their connectors, and the communication protocol already need to be defined in the configuration phase. The mapping function of the Advanced Adapter Engine then only statically controls the exchange of messages between the predefined connectors of the communication partners, which increases performance.

- **Direct communication bypassing the PI Integration Server**
  SAP NetWeaver PI also dynamically supports web service communication directly between the WS provider and the consumer without PI Integration Server or the Advanced Adapter Engine. This option is configured in the PI Integration Directory and allows for an increased message throughput.

To describe the preceding PI components, the following sections provide further information on the logical technical PI architecture. If SAP NetWeaver PI is used, three phases are supported: the design phase, the configuration phase, and the runtime phase (see Figure 12.1).

- **Design time**
  During the design phase, the Enterprise Services Builder/Integration Builder is used to define, design, and store the integration components and web services in the Enterprise Services Repository or Services Registry. The Services Registry corresponds to Universal Description, Discovery and Integration (UDDI) Standard 3.0 and plays a central role in provisioning web services. The Integration Directory is used to model the Application-to-Application (A2A) and Business-to-Business (B2B) communication processes.

- **Configuration time**
  The configuration phase involves further configuration of the integration scenario as defined in the Integration Directory. During this phase, communication partners, communication components, and communication channels are configured in communication profiles as defined in the Integration Directory. This includes controls, such as the mapping of senders/recipient, the routing
of messages, or the monitoring of the processes. The Business Process Engine, Integration Engine, and Advanced Adapter Engine, which support process integration for the runtime, are the essential Integration Server components.

![Diagram of Implementation Phases in SAP NetWeaver PI](image)

**Figure 12.1** Implementation Phases in SAP NetWeaver PI

**Runtime**

At runtime, the communication profiles and integration rules as defined in the Integration Directory are used for process integration by the Integration Server components (Business Process Engine, Integration Engine, and Advanced Adapter Engine). The Integration Engine is responsible for the control, processing, and monitoring of web services, and the Advanced Adapter Engine provides numerous connectors for supporting the direct integration of communication between heterogeneous applications. This often requires a conversion of the communication protocols through the Advanced Adapter Engine. The Business Process Engine implements the process integration at runtime, controls the business process flow, and supports the monitoring processes.

The System Landscape Directory (SLD) stores all metadata that describes the necessary components, adapter versions, and so on. This data is read and updated at runtime, if necessary, by the other PI components, such as the Enterprise Services Repository, Integration Directory, and Integration Server.
From a security validation perspective, the following aspects are therefore particularly essential:

- A direct interaction of a user with SAP NetWeaver PI only takes place during the design and configuration time. Afterward, the processes run automatically in the runtime environment and must be monitored appropriately via monitoring processes. The configuration data stored in the SLD, Enterprise Services Repository, and Integration Directory is only accessed by authenticated administration users during the design and configuration phase.

- The security level to be achieved at runtime, particularly the security of exchanged messages by digital signature and encryption, is specified in the collaboration agreements. This is achieved by receiver agreements specifying that a message is to be encrypted and signed before it can be sent to the final recipient. In the same manner, the sender agreements can define that a signature of an inbound message needs to be validated before the message can be processed further. This holds true whether an application is a sender, or a recipient is always determined by the respective communication partner and not in SAP NetWeaver PI. An application sending a message to the PI system is therefore a sender.

- SAP NetWeaver PI consists of numerous components exchanging information with each other. Mutual authentication is implemented via one-factor authentications based on technical users. Process integration, on the basis of the enterprise service bus using web services, requires that security criteria like authentication, authorization checks, data integrity, and data protection can be used for service-oriented architectures. To meet these criteria and control objectives, the corresponding security concepts are available for web services.

12.2 Risks and Controls

SAP NetWeaver PI runs on the SAP NetWeaver AS and uses it at runtime. The two usage types, ABAP and Java, involve similar risks that can also be mastered with the same controls.

In this section, we use a simplified version of the risk analysis methodology described in Chapter 1, Risk and Control Management, to identify the main security risks and the necessary controls for SAP NetWeaver PI (see Table 12.1). The controls are then discussed in more detail in the following sections and illustrated using examples.
### Table 12.1 Risks and Controls for SAP NetWeaver PI

<table>
<thead>
<tr>
<th>No.</th>
<th>Classification</th>
<th>Description</th>
<th>Impact</th>
<th>Risk without control(s)</th>
<th>Control</th>
<th>Risk with control(s)</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Risk potential</td>
<td>No authorization concept for the design and configuration phase: Via the Enterprise Services Builder, users can access configurations for which they are not authorized. This is enabled by a nonexistent or insufficient authorization concept.</td>
<td>The configuration of the integration scenario causes it to become unstable, leaving message exchange vulnerable to being impaired and manipulated. The availability of the integration platform can no longer be guaranteed. Message recipients can also be changed so that required postings are not affected in the actual target system, but in a system intended for this purpose by a fraudulent user.</td>
<td>Extremely high</td>
<td>Adequate roles are specified for accessing objects and collaboration agreements stored in the Enterprise Services Repository and Integration Directory. This is set in an authorization concept.</td>
<td>Normal</td>
<td>12.3.1</td>
</tr>
<tr>
<td>2.</td>
<td>Risk potential</td>
<td>Passwords that are too simple: Passwords and authorizations for technical service users, which are necessary for authentication among the RFC communication partners, are too simple and can be discovered easily.</td>
<td>If insufficient authentications or incorrect authorizations are selected for technical service users, the component can be accessed directly, and therefore the configuration can be changed by unauthorized persons. This jeopardizes the configuration stability and availability of SAP NetWeaver PI. Unauthorized users can also read and manipulate component information.</td>
<td>High</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No.</td>
<td>Classification</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>----------------</td>
<td>-------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control</td>
<td>The passwords for technical service users must be secure, that is, they must have sufficiently complex characteristics. Default passwords must be changed in any case. In addition, the authorizations of technical service users must be determined in accordance with the predefined roles.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk with control(s)</td>
<td>Normal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Section</td>
<td>12.3.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Risk potential</td>
<td>Missing authorization concept for the SAP NetWeaver PI components: Via the Services Registry or UDDI server, users can access service definitions and configurations for which they are not authorized.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Impact</td>
<td>The configuration of the central SAP NetWeaver PI components becomes unstable, leaving Services Registry vulnerable to being impaired and manipulated. The availability of the services can no longer be guaranteed. Service definitions can also be changed so that required postings are not affected in the actual target system, but in a system intended for this purpose by a fraudulent user.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk without control(s)</td>
<td>Extremely high</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control</td>
<td>Respective roles are specified for administrative access to the services in Services Registry. This is set in an authorization concept.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk with control(s)</td>
<td>Normal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Section</td>
<td>12.3.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Risk potential</td>
<td>Passwords that are too simple: The authentication mechanism for administrative access to SAP NetWeaver PI components is based on the user ID and password method. The password is too simple.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Impact</td>
<td>Unauthorized users can gain access by guessing the password in a brute-force attack. This allows them to compromise the service configuration.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk without control(s)</td>
<td>Extremely high</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 12.1  Risks and Controls for SAP NetWeaver PI (Cont.)
<table>
<thead>
<tr>
<th>No.</th>
<th>Classification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Control</td>
<td>Selection of an appropriately complex password for the authentication of administrators</td>
</tr>
<tr>
<td></td>
<td>Risk with control(s)</td>
<td>Normal</td>
</tr>
<tr>
<td>Section</td>
<td>12.3.4</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Risk potential</td>
<td>The selected technical service user is the same: The same technical service user (PIAPPLUSER) is used for all communication channels from different SAP systems to the PI server. There is no differentiation of the different SAP systems.</td>
</tr>
<tr>
<td>Impact</td>
<td></td>
<td>Because there is no differentiation, other communication channels of SAP NetWeaver PI can be used by other SAP systems as well. Unauthorized transactions can therefore be triggered on other connected SAP systems.</td>
</tr>
<tr>
<td>Risk without control(s)</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>Control</td>
<td>For every SAP NetWeaver AS system communication channel via RFC, HTTP, and so on, a different technical system user with another password should be selected.</td>
<td></td>
</tr>
<tr>
<td>Risk with control(s)</td>
<td>Normal</td>
<td></td>
</tr>
<tr>
<td>Section</td>
<td>12.4.1</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Risk potential</td>
<td>No encryption of communication channels: Communication channels to the PI server transferring authentication data of technical service users for the communication channel are not encrypted. Furthermore, the communication channels to the connected partner systems that are supposed to be integrated are also not encrypted.</td>
</tr>
<tr>
<td>Impact</td>
<td></td>
<td>The authentication data of technical service users can be eavesdropped, and therefore, can be used by unauthorized communication partners connected to the PI system. The unencrypted external communication channels enable third parties to view the exchanged messages and gain insight into confidential data. In addition, unauthorized financing transactions might be effected.</td>
</tr>
<tr>
<td>Risk without control(s)</td>
<td>Extremely high</td>
<td></td>
</tr>
</tbody>
</table>

*Table 12.1* Risks and Controls for SAP NetWeaver PI (Cont.)
<table>
<thead>
<tr>
<th>No.</th>
<th>Classification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control</td>
<td>The internal communication channels between the SAP NetWeaver PI components must be encrypted. The communication channels between SAP and non-SAP systems connected to SAP NetWeaver PI should be secured via encryption techniques, such as (SSL) or (SNC).</td>
<td></td>
</tr>
<tr>
<td>Risk with control(s)</td>
<td>Normal</td>
<td></td>
</tr>
<tr>
<td>Section</td>
<td>12.4.2</td>
<td></td>
</tr>
</tbody>
</table>

### 7. Risk potential

No signature of XML messages:

XML-based messages (per XI or SOAP protocol) are submitted unsigned to SAP NetWeaver PI and forwarded as such to the actual recipient.

#### Impact

The problem with unsigned messages is that you can't verify the identity of the exact sender, nor can you check whether parts of the message were changed by a third person during the transfer to SAP NetWeaver PI. Moreover, incorrect postings can be triggered. Also, you can't retrace who initiated the financing transaction as completed transactions can later be denied by the sender.

Risk without control(s) Extremely high

Control All inbound XML-based messages must be digitally signed by the sender, especially when using SAP NetWeaver PI in Internet scenarios where business partners are supposed to be integrated.

Risk with control(s) Normal

Section 12.4.3

### 8. Risk potential

No encryption of external communication channels:

XML-based messages (per XI or SOAP protocol) are transferred unencrypted to SAP NetWeaver PI.

#### Impact

If XML-based messages are transferred unencrypted to SAP NetWeaver PI, the information contained therein can be recorded (sniffed) by unauthorized third persons. If the information is highly confidential, that is, secret business information, the damage potential is accordingly high.

Table 12.1 Risks and Controls for SAP NetWeaver PI (Cont.)
<table>
<thead>
<tr>
<th>No.</th>
<th>Classification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Risk without control(s)</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Control</td>
<td>The messages should be encrypted, especially when using SAP NetWeaver PI for integration scenarios where business partners have to be integrated via the Internet, and where the business data is highly confidential.</td>
</tr>
<tr>
<td></td>
<td>Risk with control(s)</td>
<td>Normal</td>
</tr>
<tr>
<td></td>
<td>Section</td>
<td>12.4.4</td>
</tr>
</tbody>
</table>

9. Risk potential The SAP NetWeaver PI communication channels are not secured:
Communication interfaces of SAP NetWeaver PI, particularly in Internet scenarios, are abused by unauthorized third persons. Therefore, unauthorized transactions are triggered on the SAP and non-SAP systems to be integrated via SAP NetWeaver PI.

Impact If unauthorized transactions are executed, you can't retrace who initiated them. Rollback — restoring the original state — is also not possible, which can result in considerable damage.

| Risk without control(s) | Extremely high |
| Control | A proxy for outbound messages and a reverse proxy for inbound messages should be implemented for SAP NetWeaver PI. Particularly in Internet scenarios, two consecutive PI systems located in different network segments should be used. One in the front-end demilitarized zone for communicating with business partners (B2B) and another one for the back-end for the internal A2A communication. |
| Risk with control(s) | Normal |
| Section | 12.4.5 |

10. Risk potential The message exchange is not audited or monitored:
The executed messages and transactions are not checked for potential processing errors by the central monitor.

Table 12.1 Risks and Controls for SAP NetWeaver PI (Cont.)
<table>
<thead>
<tr>
<th>No.</th>
<th>Classification</th>
<th>Description</th>
<th>Risk without control(s)</th>
<th>Control</th>
<th>Risk with control(s)</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Impact</td>
<td>Processing errors are not discovered at an early stage and therefore result in instabilities in the integration network. In short, transactions that weren’t executed properly cannot be determined in time, which, in turn, can lead to financial losses.</td>
<td>High</td>
<td>Constant monitoring of SAP NetWeaver PI using the central monitor provided for this purpose.</td>
<td>Normal</td>
<td>12.4.6</td>
</tr>
<tr>
<td>11.</td>
<td>Risk potential</td>
<td>No authentication for the file adapter: SAP NetWeaver PI lets you retrieve files from a sending system and to place them on a receiving system using file adapters. There is no authentication for the file adapter — at a technical or user level. This communication channel, therefore, is easily accessible.</td>
<td>High</td>
<td>It is vital that you ensure a correct configuration of authorizations at the operating system level for the relevant file directories, especially when using the file adapter. In particular, this applies to the SYSADM user, under whose tutelage SAP NetWeaver PI is executed.</td>
<td>Normal</td>
<td></td>
</tr>
<tr>
<td>12.</td>
<td>Risk potential</td>
<td>No encryption of communication channels: The communication channels between the SAP NetWeaver PI components and the connected partner systems are not encrypted.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 12.1  Risks and Controls for SAP NetWeaver PI (Cont.)
Table 12.1 Risks and Controls for SAP NetWeaver PI (Cont.)

<table>
<thead>
<tr>
<th>No.</th>
<th>Classification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.</td>
<td>Risk potential</td>
<td>Web service security options are not utilized: Web services and enterprise services are not protected against their integrity and confidentiality being compromised.</td>
</tr>
<tr>
<td></td>
<td>Impact</td>
<td>Unprotected service message can make confidential business data public. In addition, data might be changed or unauthorized financing transactions triggered.</td>
</tr>
<tr>
<td></td>
<td>Risk without control(s)</td>
<td>Extremely high</td>
</tr>
<tr>
<td></td>
<td>Control</td>
<td>Web service security needs to be optimally configured considering the technical options.</td>
</tr>
<tr>
<td></td>
<td>Risk with control(s)</td>
<td>Normal</td>
</tr>
<tr>
<td></td>
<td>Section</td>
<td>12.4.9</td>
</tr>
</tbody>
</table>

12.3 Application Security

This section describes in more detail the risks and controls that are outlined in Table 12.1 with regard to application security.

12.3.1 Authorizations for Enterprise Services Builder

SAP NetWeaver PI does not involve direct interaction with the users in the departments at runtime. SAP NetWeaver PI is pure middleware or back-end infrastructure that transports messages from one SAP or non-SAP system to another target system. Using appropriate mapping rules, messages can be converted and trans-
lated so that they're understood by the receiving system. SAP NetWeaver PI therefore fulfills the function of a central integration hub for all applications connected via connectors.

The only interaction between SAP NetWeaver PI and users, except for monitoring, takes place during the design and configuration phase. Using the Enterprise Services Builder/Integration Builder, these administrative users access the Enterprise Services Repository, Integration Directory, and SLD. A part of the user authorization is performed on the AS ABAP and can therefore be defined via the ABAP authorization system. The Enterprise Services Builder is a Java application where access to single objects of the Integration Directory can be authorized.

SAP delivers the following standard roles for administration (design and configuration phase) that can be used in this respect:

- **SAP_XI_DISPLAY_USER**
  This role only grants the user read access to the information contained in the Enterprise Services Repository and Integration Directory (integration objects, communication interfaces, and so on).

- **SAP_XI_DEVELOPER**
  This role can create, delete, and change the integration components in the Enterprise Services Repository.

- **SAP_XI_CONFIGURATOR**
  This role can create, delete, and change integration scenarios in the Integration Directory.

- **SAP_XI_CONTENT_ORGANIZER**
  This role can create, delete, and change the contents in the SLD.

- **SAP_XI_MONITOR**
  This role can monitor all SAP NetWeaver PI components and all messages that were processed using SAP NetWeaver PI.

- **SAP_XI_ADMINISTRATOR**
  This role includes all roles mentioned and is thus a master role for SAP NetWeaver PI administration.

Access to the individual object types within the Enterprise Services Repository and Integration Directory can, as mentioned earlier, be designed in a more detailed way. To do this, the following conditions must be met:

- **The J2EE parameter in the Exchange profile, com.sap.aii.ib.server.lock-auth.activation, found at http://<server>:<HTTP port>/exchangeProfile, must be set to true.**
On the AS ABAP of the PI system, the **SAP_XI_ADMINISTRATOR_J2EE** role must be assigned to the administrator, because it grants access to the Enterprise Services Builder role configurator, which is available in the Enterprise Services Builder menu. This ABAP role must therefore be granted in a very restrictive way.

Using this role configurator, accesses within the Enterprise Services Builder to the object types can be limited in both the Enterprise Services Repository and in the Integration Directory. In the Enterprise Services Repository, access to individual software component versions, name ranges, and repository object types (software components, integration scenario objects, interface objects, mapping objects, adapter objects, and imported objects) can be limited. The authorizations to Create, Change, and Delete can be granted.

In the Integration Directory, the access to the object types Interface Determination, Recipient Determination, Receiver Agreement, Configuration Scenario, and Special Agreement can be restricted. To do this, the authorizations to Create, Change, and Delete are also available. In general, read access is granted using the **SAP_XI_DISPLAY_USER** ABAP role.

If new roles are created for the Enterprise Services Builder, the corresponding roles are physically stored in the UME (see Chapter 9, SAP NetWeaver AS). These UME roles for the Integration Repository then start with **XIRep_***, or **XIDir_*** for the Integration Directory. In the UME, they can either be assigned directly to the existing administrator or to a user group.

**Note**

Please remember: The UME group name is identical to the name of the ABAP role. Therefore, if you assigned a specific role in the AS ABAP to a specific person group, this ABAP role can be addressed as a group in the UME. In the same way, the defined Enterprise Services Builder UME roles can be assigned to the same ABAP users.

### 12.3.2 Passwords and Authorizations for Technical Service Users

The various SAP NetWeaver PI components listed previously, like Enterprise Services Repository, Integration Directory, Integration Server, and so on, must access one another during the design, configuration, and runtime phases, for example, to read or write information. During this access, a component; for example, the Integration Directory accessing the Integration Server, reads the relevant technical service user data from the Exchange profile, in this case **PIIUSER**, and then uses it to authenticate itself to the Integration Server. The service user data is read from **PIIUSER** via the **PILDUSER** service user that knows every component.
The following technical service users are used to access the respective component:

- **Exchange profile and System Landscape Directory**
  Access via the technical service user PILUSER using the ABAP role SAP_BC_AI_LANDSCAPE_DB_RFC.

- **Enterprise Services Repository**
  Access via the technical service user PIREPUSER using the ABAP role SAP_XI_IR_SERV_USER.

- **Integration Directory**
  Access via the technical service user PIDIRUSER using the ABAP role SAP_XI_ID_SERV_USER.

- **(Advanced) Adapter Engine**
  Access via the technical service user PIAFUSER using the ABAP role SAP_XI_AF_SERV_USER_MAIN.

- **Integration Server**
  Access via the technical service user PIISUSER using the ABAP role SAP_XI_IS_SERV_USER_MAIN.

- **Runtime Workbench (cache at runtime)**
  Access via the technical service user PIRWBUSER using the ABAP role SAP_XI_RWB_SERV_USER_MAIN.

These technical service users are set up during the SAP NetWeaver PI installation and are automatically configured. The passwords need to be chosen during the installation, and it is critical that they are sufficiently complex. The following rules should be applied:

- Password length to be a minimum of eight characters
- At least one special character
- At least one letter
- At least one number

### 12.3.3 Authorizations for Administrative Access to SAP NetWeaver PI

SAP NetWeaver PI can be considered middleware that only administrative employees need to access for configuration or monitoring tasks. Although access is therefore granted to a limited number of people, an authorization concept that assigns appropriate and restrictive authorizations needs to be documented and used.
For the essential SAP NetWeaver PI components, the standard version provides predefined ABAP roles of which — according to Best Practices — copies are adapted to the specific requirements and assigned to the administrative user. The following rules are available for the three components:

- **Enterprise Services Repository**
  - **SAP_XI_ADMINISTRATOR_J2EE** (administrative access to the AS Java)
- **Enterprise Services Registry**
  - **SERVICES_REGISTRY_READ_ONLY** (read-only access to the Services Registry)
  - **SERVICES_REGISTRY_READ_WRITE** (read access to all classifications and write access to classifications that are not predefined or technical)
  - **SERVICES_REGISTRY_BUSINESS_ADMINISTRATOR** (read access to all classifications and write access to classifications that are not technical)
  - **SERVICES_REGISTRY_TECHNICAL_ADMINISTRATOR** (read and write access)
- **Universal Description, Discovery, Integration (UDDI) server**
  - **UDDI_Admin** (object administration, access to user information)
  - **UDDI_TierN** (object administration, no access to user information)
  - **UDDI_Tier1** (service administration, no access to user data)

### 12.3.4 Password Rules for Administrators

It is important that administrators have separate, individual user names and passwords for SAP NetWeaver PI. This is an administrator’s individual responsibility. Password rules should be generally applicable and specify that passwords need to be sufficiently complex:

- Password length to be a minimum of eight characters
- At least one special character
- At least one letter
- At least one number

### 12.4 Technical Security

This section describes in more detail the risks and controls that are outlined in Table 12.1 with regard to technical security.
12.4.1 Definition of Technical Service Users for Communication Channels at Runtime

At runtime, there are different communication channels that are used to access SAP NetWeaver PI. For these communication channels, an authentication is performed using technical service users.

**Scenario 1: Communication between Sending System and Integration Server via the XI Protocol**

In one important scenario, the sender is an SAP NetWeaver AS (Release 6.20 or higher). In this case, an ABAP application can send a message via the ABAP proxy using the XI protocol. A service user `PIAPPLUSER` then needs to be set up on the Integration Server that enables the SAP NetWeaver AS to log on to the Integration Server. In the ABAP stack, it has the `SAP_XI_APPL_SERV_USER` role.

For every SAP NetWeaver AS that is logged on, a separate technical service user, `PIAPPLUSER`, needs to be configured. The technical service user `PIAPPLUSER` is also used when the sending SAP NetWeaver AS connects to the Integration Server via RFC or IDocs. Communication with the recipient (SAP NetWeaver AS) via the XI protocol requires a technical service user as well.

**Scenario 2: Communication between Sending System and Integration Server via the Adapter Engine and Various Adapters**

For communication between a sending SAP and non-SAP system via an adapter, the authentication scheme that is necessary for the relevant adapter type is used — usually via technical service users. When using a file, database, or Java Message Service (JMS) adapter, `PIAFUSER` is used. The Adapter Engine (either central or decentralized) communicates with the Integration Server using the technical service user `PIISUSER` via the XI protocol. The technical service user `PIISUSER` must be assigned the ABAP role `SAP_XI_APPL_SERV_USER_Main` as well. For communication between the Integration Server and the Adapter Engine, the initial authentication is performed using `PIAFUSER`, which must be assigned the role `SAP_XI_APPL_SERV_USER_Main` for this purpose. The subsequent communication to the final recipient depends on the respective adapter.

**Changing the Passwords for Service Users**

The passwords used for the technical service users must be changed regularly, at least once a year. This is critical to support password security and to make sure that attempts at decrypting the password are not successful. You make this change
in the Exchange profile, which can be called via the following: \texttt{http://host:port/exchangeProfile}.

The password must be changed in the corresponding entry \texttt{com.sap.aii.<component>.serviceuser.pwd} (for example, \texttt{com.sap.aii.integration_directory.serviceuser.pwd} for the Integration Directory). This must also be done in the corresponding entry in the AS ABAP for the technical service user as well using Transaction SU01.

12.4.2 Setting Up Encryption for Communication Channels

As mentioned earlier, SAP NetWeaver PI lets you distinguish between the internal communication based on technical service users and the external communication to the connected partner systems. The internal communication among the components takes place via HTTP, which can be secured using SSL (or HTTPS, respectively).

When securing the external communication channels, the encryption type depends on the adapter. For adapters where the protocol used for communication is also based on HTTP, HTTPS can be implemented as well. For communication interfaces based on RFC, SNC can be used.

In general, an encrypted SSL or SNC communication can be configured in the same way as the SAP NetWeaver AS, because SAP NetWeaver PI is built on this technical runtime environment. As a general prerequisite for using SSL, the necessary cryptographic program libraries (for example, SAPCRYPTOLIB for ABAP and the IAIK security package for J2EE) must be installed in both AS ABAP and AS Java. In both cases, the appropriate digital certificates (according to X.509 standard) must be requested by a Certificate Authority (CA). Because SSL is also used for technically authenticating two communication partners, it can be configured so that the server not only authenticates itself to the client but that the client also authenticates itself to the server. In internal PI communication, the components partially function as client and server.

The SSL (HTTPS) communication must therefore be configured for both stacks (AS ABAP and AS Java):

- For AS ABAP, Transaction STRUST must be used to configure the SAP NetWeaver AS for SSL and used for SAP NetWeaver PI; this is where the digital certificate mentioned must be imported. In addition, an appropriate HTTPS service with one port must be set up for the ICM (Transaction SMICM, services).
For the AS ABAP to function as a client as well, the digital certificate must be imported in the client Personal Security Environment (PSE) using Transaction STRUST. This can be the same client that was used for the server as well. Otherwise, the HTTPS port of the respective server must be used for all destinations (Transaction SM59) where HTTPS with client authentication is to be used.

In addition, AS Java must be adequately configured as an HTTPS server. This is done using the Visual Administrator. The requested certificate must be imported into the key store service_ssl under the Key Storage provider. Also, the certificate must be assigned to the HTTPS service in the SSL provider, and the port for HTTPS must be configured and activated.

In order for AS Java to act as a client, in addition to importing the server certificate to the service_ssl key store, it must also be imported to the TrustedCAs key store if self-signed certificates will be used.

**Configuration of the Internal PI Communication**

To change the entire internal communication to SSL (HTTPS), you must set the following parameters in the Exchange profile:

- The `com.sap.aii.connect.secure_connections` parameter must be set to all.
- The parameters defining the HTTPS communication ports (for example, `com.sap.aii.connect.integrationserver.httpsport`) must be set to the port that has been defined for the HTTPS service — either AS ABAP or J2EE, depending on the technical runtime environment of the component.

More information about configuring a secure internal PI communication can be found in SAP Note 766215.

**Configuration of External Communication**

For the external communication of messages via the communication channels defined in the Integration Directory, the implementation depends on the relevant carrier protocol. If it is the commonly used HTTP, you can select the corresponding secure equivalent HTTPS in the Integration Directory (provided that the appropriate HTTPS service has been activated on the sender or receiving system, respectively, as already described). Otherwise, it depends on the adapter. For RFC adapters, the secure SNC protocol can be used instead of SSL.

Table 12.2 contains information about the most commonly used adapters and their protection options.
Adapter | Runs on | Outbound | Inbound | Protocol | Protection |
--- | --- | --- | --- | --- | --- |
XI | IS | X | | HTTP | Possible via HTTPS. This is achieved with the selection via the encrypted communication channel in the Integration Directory. |
| | | X | | HTTP | Possible via HTTPS. This is achieved with the selection via the encrypted communication channel in the Integration Directory. |
IDoc | IS | X | | tRFC | Possible via SNC. The connection must be defined with a technical service user as a communication channel of the IDoc type. The channel must reference an appropriate RFC connection (type 3) between SAP NetWeaver PI and the receiving system (IDoc). The technical service user in the receiving system (IDoc) must have the corresponding IDoc authorizations. |
| | | X | | | Possible via SNC. The connection must be defined as a type-3 RFC destination on the sending IDoc system. The technical service user must have the `SAP_XI_APPL_SERV_USER` role in SAP NetWeaver PI. |

Table 12.2 External Adapters and Encryption Possibilities for the Relevant Communication Protocols
<table>
<thead>
<tr>
<th>Adapter</th>
<th>Runs on</th>
<th>Outbound</th>
<th>Inbound</th>
<th>Protocol</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plain HTTP IS X HTTP</td>
<td>Possible via HTTPS. In the Integration Directory, the communication channel type HTTPS must be selected. Depending on the configuration of the target system, an anonymous login or the authentication using a technical service user is permitted.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>HTTP</td>
<td>Possible via HTTPS. To address this adapter, the sender must address the PI system (Integration Directory) via the <code>https://&lt;XI host&gt;:&lt;HTTPS port&gt;/sap/xi/adapter_plain</code> service. An authentication scheme must be stored in the service (to be set via Transaction SICF). The technical service user must have the <code>SAP_XI_APPL_SERV_USER</code> role.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RFC AE X RFC</td>
<td>SNC is not possible. In the Integration Directory, only the RFC type can be selected for the communication channel. For this purpose, an appropriate RFC connection (Transaction SM59) must be set up between the Integration Server and the receiving system.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 12.2** External Adapters and Encryption Possibilities for the Relevant Communication Protocols (Cont.)
Adapter | Runs on | Outbound | Inbound | Protocol | Protection
---|---|---|---|---|---

The RFC service user must have the corresponding authorizations in the receiving system. (Note: This adapter should only be implemented in an intranet scenario.)

X | RFC | SNC is not possible. You must define an RFC connection from the Integration Server back to the actual target system that can be used to read the RFC metadata. To do this, the adapter should be registered accordingly with the SAP Gateway. There is no authentication via a technical service user. (Note: This adapter should not be implemented in an Internet scenario.)

SOAP | AE | X | HTTP | Possible via HTTPS. In the Integration Directory, SOAP needs to be defined for the receiving channel. The channel can be authenticated to the receiving application using a technical service user. An anonymous login is permitted as well. In addition, the message can be digitally signed.

Table 12.2  External Adapters and Encryption Possibilities for the Relevant Communication Protocols (Cont.)
Adapter Runs on Outbound Inbound Protocol Protection

<table>
<thead>
<tr>
<th>Adapter</th>
<th>Runs on</th>
<th>Outbound</th>
<th>Inbound</th>
<th>Protocol</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>HTTP</td>
<td>Possible via HTTPS. In the sending channel of the Integration Directory, SOAP must be set. The corresponding technical service user can be authenticated via basic authentication or SSL client certificate. This technical service user requires the xi_adapter_soap_message role in the Adapter Engine. This must be set via the UME. The signature validation of the message can be enabled as well.</td>
</tr>
<tr>
<td>Rosetta Net InterFace (RNIF)</td>
<td>AE</td>
<td>X</td>
<td></td>
<td>HTTP</td>
<td>Possible via HTTPS. In the Integration Directory, the RNIF type needs to be defined for the receiving channel. The channel can be authenticated to the recipient using a technical service user. An anonymous login is permitted as well. In addition, the message can be digitally signed and encrypted.</td>
</tr>
</tbody>
</table>

Table 12.2 External Adapters and Encryption Possibilities for the Relevant Communication Protocols (Cont.)
### Table 12.2 External Adapters and Encryption Possibilities for the Relevant Communication Protocols (Cont.)

<table>
<thead>
<tr>
<th>Adapter</th>
<th>Runs on</th>
<th>Outbound</th>
<th>Inbound</th>
<th>Protocol</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chemical Industry Data Exchange (CIDX)</td>
<td>AE</td>
<td>X</td>
<td></td>
<td>HTTP</td>
<td>Possible via HTTPS. Use the same options as for the RNIF adapter.</td>
</tr>
<tr>
<td>File system</td>
<td>AE</td>
<td>X</td>
<td></td>
<td>NFS</td>
<td>There are security options only at the operating system level. For the SYSADM technical user that runs the PI instance, access to operating system directories must be restricted. There are no encryption options. Using this adapter is not recommended in scenarios with very high security requirements.</td>
</tr>
</tbody>
</table>

The technical service user requires the SAP_XI_APPL_SERV_USER role in AS ABAP. A signature validation of the message can be enabled as well. In addition, the message can be decrypted.

Using this adapter is not recommended in scenarios with very high security requirements.
<table>
<thead>
<tr>
<th>Adapter</th>
<th>Runs on</th>
<th>Outbound</th>
<th>Inbound</th>
<th>Protocol</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td>AE</td>
<td>X</td>
<td></td>
<td>FTP</td>
<td>Secure FTP is not possible. Apart from that, you can also use technical service users for FTP authentication. We do not recommend using FTP for integration scenarios with high security demands.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>FTP</td>
<td>X</td>
</tr>
<tr>
<td>JDBC</td>
<td>AE</td>
<td>X</td>
<td></td>
<td>JDBC</td>
<td>Depending on the manufacturer, database access might be encrypted. The authentication is again implemented using technical service users at the database level. We do not recommend using JDBC for integration scenarios with high protection needs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>JDBC</td>
<td>X</td>
</tr>
</tbody>
</table>

Table 12.2 External Adapters and Encryption Possibilities for the Relevant Communication Protocols (Cont.)
Adapter | Runs on | Outbound | Inbound | Protocol | Protection
---|---|---|---|---|---
Mail | AE | X | IMAP4, POP3, SMTP | Possible via SSL. Except for IMAP4, S/MIME, that is, the signature and encryption option for emails, can be implemented as well.

Table 12.2 External Adapters and Encryption Possibilities for the Relevant Communication Protocols (Cont.)

In general, the protection needs for the integration scenario should be determined based on SAP NetWeaver PI when selecting possible adapters. For high protection needs — for example, when connecting systems that are processing highly confidential information and information with high integrity demands — you should only implement those adapters that support digital signatures (high integrity) and encryption (high confidentiality) at the message level.

12.4.3 Digital Signature for XML-Based Messages

XML-based messages, like those used for the XI protocol, SOAP, RNIF, and CIDX adapters, can be signed. By digitally signing a message, you can achieve the following security objectives:

- The sender of a message can be unambiguously authenticated at the message level. It is not necessary to rely on the authentication of the communication channel via technical service users, because it may have been compromised by an attacker. In a purely technical authentication, it is impossible to retrace the sender in a legally binding way.

- Using a digital signature, the integrity of the message can be unambiguously determined. An unauthorized change to the message carried out by an attacker at a later stage can be discovered. If the message was changed by an attacker, SAP NetWeaver PI can refuse to process it further.

- A digital signature attests the originality of the message. A sender cannot discard sending the message at a later stage. This is particularly important if business orders are digitally processed. However, you must consider the legal requirements that are to be applied to the business contract. If you want to set
up a legal-proof contract, the signature must comply with the policies of the Electronic Signatures in Global and National Commerce Act. Naturally, this can be circumvented if the business partners have not made any other previous agreements.

Using the XI protocol, you can digitally sign the SAP manifest (part of the XI protocol with information on the processing of the message, and logistic information) and the payloads (that is the actual message), in addition to the SAP main header (similar to the SOAP header in web services). Using SOAP, however, you can only sign the SOAP body (the message only). The RNIF connector uses S/MIME, and CIDX uses the PKCS#7 signature standard.

In SAP NetWeaver PI, messages can be signed using the certificates existing in the certificate store of AS Java (key storage provider) in the PI runtime environment of the underlying SAP NetWeaver AS. The certificate store of AS ABAP is not used in this case. The Integration Server using AS ABAP as the technical runtime environment implements an internal web service for addressing the signature functions of AS Java.

For digital signatures, you must consider the trust model to be applied. There are two variants that can be implemented in this respect:

- There is a direct trust model that does not use a certificate authority: The public keys (certificates) of the sender and the recipient (of the business partners or internal systems) must be exchanged beforehand. In this case, a new key store can be created on the J2EE Engine of SAP NetWeaver PI, where all public certificates of the possible senders are stored. This key store can be freely chosen.

- A public key infrastructure is used: In this case, there is a trust relationship between the business partners that is confirmed by one or more trustworthy certificate authorities. All implemented certificates of the business partners must be digitally signed by these root certificate authorities. The relevant public certificates of the CAs must be stored in the TrustedCAs key store of AS Java. However, SAP NetWeaver PI does not support multilevel hierarchical trust relationships. Therefore, the certificates must have been signed directly by the trustworthy certificate authorities. A multilevel certificate hierarchy is not supported.

In order for the access to the key storage provider of AS Java to function correctly, you must assign the appropriate J2EE roles in AS Java (see Chapter 9) to the technical service user (RFC user), which is used by the web service (HTTP carrier protocol) to log on to the Integration Server. This is done using the Security Provider service in the Visual Administrator and affects the following roles:

- On the Policy Configuration tab, the sap.com/tc-sec-wssec-app*wssprocess.jar component needs to be selected. It contains the J2EE role WSSecurityProcess-
If a new key store has been generated for storing the external business partner system certificates, the aforementioned RFC service user must be assigned to the J2EE role KeystoreAdministrator, which is included in the keystore-view.<name of the created key store> component.

To use the J2EE security functions, the IAIK cryptography components first need to be implemented in AS Java. This is done using the software deployment tool. The collaboration agreements for communication partners that have been stored in the Integration Directory define whether it’s necessary to use digital signatures and specify the validation of a signature.

![Image of receiver agreement](image.png)

**Figure 12.2 Receiver Agreement — Signature of a Message in the Case of an XI Protocol**

The receiver agreement (see Figure 12.2) in the Integration Directory defines whether a message is signed before it is forwarded to the recipient in SAP NetWeaver PI. In this receiver agreement, the key store of AS Java is selected with

```
Receiver Communication Channel: Message_be_XI
Certificate For Signing:
  Keystore:
  Keystore Entity:
```
the corresponding signature certificate (private certificate of the Integration Server). As a prerequisite, either the XI protocol or SOAP (or RNIF or CIDX, respectively) must have been chosen for the communication channel with the recipient.

In the communication channel, Message Security should be set for the XI protocol, for example, Message_to_XI. In the key store, you specify the Key Store Name, and the key store entry contains the actual certificate. In the communication channel, the Message Security checkbox must be selected (see Figure 12.3) to enable a digital signature in the receiver agreement.

![Figure 12.3 Message Security Option for the Communication Channel of the XI Protocol](image)

The sender agreement (see Figure 12.4) in the Integration Directory specifies the public certificate of the sender to be used for validating the signed message in SAP NetWeaver PI. For self-signed certificates, the public certificates must have been imported into the key storage of AS Java. The self-signed public certificate must also have been imported to the TrustedCAs key store. The same applies to the public certificate of the certificate authority that signed the business partner system...
certificates. In the sender communication channel, the MESSAGE SECURITY option must be set. Therefore, the following must be specified:

- The communication channel with Message Security set for the XI protocol
- The issuer (certificate authority) and the owner of the certificate
- The key store Key Store Name in the J2EE stack

Because SAP NetWeaver PI can only sign using server-based certificates, there might be legal problems if more sophisticated signature policies according to the Electronic Signatures in Global and National Commerce Act are observed. To do this, SAP provides direct signature options using SAP GUI (see Chapter 28, User Interfaces).
12.4.4 Encryption of XML-Based Messages

To encrypt XML-based message content (SOAP body), you can use the RNIF and CIDX adapters. These protocols enable encryption at the message level. They use the public certificate of the business partner system (receiving system) for encryption. You can also protect messages using the traditional method — via SSL encryption of the communication channel.

12.4.5 Network-Side Security for Integration Scenarios

Particularly when SAP NetWeaver PI is used in an Internet scenario, for the integration of a business partner (supplier, reseller, customer), for example, the scenario must be secured via the network. As with portal scenarios, a multilevel demilitarized zone (DMZ) concept must be used for network segmentation, as shown in Figure 12.5.

![Figure 12.5 DMZ Concept and Implementation of Two PI Instances in an Internet Integration Scenario](image)

In an integration scenario with business partners where the Internet is used as the network between business partners and your own enterprise, two PI systems should be implemented: one system establishing the integration with the business
partners, that is, a B2B system, and a second system for the internal application integration, an A2A integration hub. This ensures that the A2A integration channels cannot be directly accessed from the Internet. Between the B2B PI system and the A2A PI system, you can establish a dedicated communication channel that can be protected and controlled in a more optimal way.

To do this, you can use the XI protocol, which can implement an additional message signature. In addition, this communication channel can be encrypted using HTTPS. This also enables a mutual authentication at a technical level between the B2B and A2A integration systems. The firewall between DMZ 2 and the back-end may only permit communication between B2B and A2A PI systems.

If all systems (for example, SAP Partner Connectivity Kit, see Chapter 13, Partner Connectivity Kit) used by the business partners are known, the outer firewall should also restrict access to these systems. This does not prevent IP spoofing attacks, but it does provide additional protection.

For inbound messages, the communication should be directed via at least one reverse proxy. For outbound messages, from the B2B integration system to the business partner, a proxy should be implemented. We recommend that you only use XI protocol, SOAP, RNIF, and CIDX for communicating with business partners, because this is the only way to achieve good message security with digital signature and encryption. As a reverse proxy, you can use the SAP Web Dispatcher in this integration scenario, which only provides very limited security functions. Only the URL services, which must be called externally, can be restricted.

Preferable solutions would be application-level gateways (or web application firewalls) that are specifically designed for XML-based message communication, that is, web services. They provide the security functionalities necessary for a secure communication based on web services. The web services application level gateways can check the contents of the SOAP header and SOAP body for suspicious, uncommon program fragments. These kinds of program fragments are included in regular messages, for example, to bypass or eliminate the security system (see Chapter 5, Information Technology (IT) Security). In addition, these gateways provide the full range of web services security standards such as Security Assertion Markup Language (SAML) for an additional authentication or web service security.

12.4.6 Audit of the Enterprise Services Builder

The investigative security objective — within the security management — can be achieved by using an audit. An audit lets you detect changes made to the configuration or security violations and to take proper countermeasures. By using an audit, you may also find potential security weak spots that require new security controls. SAP NetWeaver PI provides numerous options for an audit.
Change History in the Enterprise Services Builder
In the Enterprise Services Builder, a change history can be called for every object in the Enterprise Services Repository and Integration Directory that has been changed. Using this change history, you can retrace who made what change to which object at what time. The change history can be called in the object's detail view by selecting History from the main menu of the object.

Monitoring Outbound Messages
The entire message processing can be monitored in the Integration Server and the Adapter Engine. There you can see if a message transfer failed, or if a recipient is still not reachable. The monitor for the Integration Server is started via Transaction SXMB_MONI (see Figure 12.6).

![Figure 12.6 SXMB_MONI in the Integration Server](image)

The administration of the Integration Server and of the archive function for processed XML messages is accessible via Transaction SXMB_ADM. The monitor for the Adapter Engine is accessible in AS ABAP via Transaction SXMB_IFR. This
transaction starts the web front end, which also activates the Enterprise Services Builder. You can start the monitoring function with a mere click on the Runtime Workbench link.

By default, only XML messages processed in an asynchronous way are made persistent in the Integration Server. XML messages that are processed synchronously are only made persistent if errors occur, or if the logging function has explicitly been switched on. Incorrect message transfers are never deleted automatically. They have to be removed manually by the administrator.

Only messages that were successfully processed in an asynchronous way can be archived or deleted. The archiving of the processed messages can be controlled using Transaction SXMB_ADM. Two archiving jobs need to be set up:

- One archiving job that writes those messages to an archive that was made persistent in the Runtime Workbench.
- One deletion job that deletes those messages that were made persistent in the Runtime Workbench.

Messages that were processed using the Message Security mode (that were digitally signed) are always archived. This applies to both messages that were asynchronously processed and to those that were synchronously processed.

Apart from mere monitoring, an alert function can be defined as well (Transaction SXMB_MONI) that triggers an alarm if messages were not correctly processed. This function can also be linked to the Computing Center Management System (CCMS) so that these alarm messages can also be reported centrally to an SAP system. The important aspect here is that a process has been defined that specifies the measures to be taken if a high-priority alarm is raised. In this case, the required countermeasures need to be initiated.

### 12.4.7 Securing the File Adapter at the Operating System Level

The file adapter provides an immense security leak, because it allows unauthorized access to the Network File System (NFS) file directories of an integration system. We strongly advise against implementing it, particularly in the context of an Internet-based integration scenario.

But, if there is no other option, you should take the appropriate security measures at the operating system level. This includes granting authorizations to the technical SYSADM user running SAP NetWeaver PI at the operating system level that enable access to only a specific file directory. On Windows-based systems, this can be done using Access Control Lists (ACLs). On UNIX systems, the correct user ID needs to be set. You should specifically define an exchange directory. All other system-critical directories must be protected using special access restrictions.
12.4.8 Encrypting PI Communication Channels and Web Services

Data networks usually have obvious security gaps when confidential data is transferred without encryption. To address the related risks, you can implement standard data encryption methods, such as SSL. This data encryption at the transport level is the simplest and a generally compatible approach for protecting data during transport from communication point to communication point (end-to-end); the AS Java supports SSL by default (see Chapter 9).

This kind of encryption, however, is usually undone when data is received in a system before it is forwarded again. This results in an additional security gap because the data remains in plain text or is stored temporarily before it is encrypted with SSL again and forwarded. You can close this security gap by also encrypting the data. The data should remain encrypted until the recipient receives it. This additional protection is recommended for web services.

To support this concept, the XML encryption standard by the Organization for the Advancement of Structured Information Standards (OASIS) (http://www.oasis-open.org) provides standardized guidelines for a direct encryption of web services (XML, SOAP). Before using this method, however, it must be ensured that all communicating systems are able to encrypt and decrypt data according to this standard.

In Release 7.1, SAP NetWeaver PI supports this standard. XML encryption is a part of the WS-Security that defines the guidelines for SOAP message authentication, digital signatures, and encryption of message texts. In Release 7.1, you configure this by performing the following steps in SAP NetWeaver Administrator:

1. You configure the default WS-Security in SAP NetWeaver Administrator via the following menu path: **SOA MANAGEMENT • WEB SERVICES ADMINISTRATION FOR WS CONFIGURATION • SERVICE END POINTS • SERVICE DEFINITION DETAILS**.

2. Afterward, you configure the PI client in SAP NetWeaver Administrator via the menu path: **SOA MANAGEMENT • WEB SERVICES ADMINISTRATION FOR WS CLIENTS CONFIGURATION • LOGICAL PORTS • PROXY DEFINITIONS DETAILS**.

3. To define SSL as the standard for clients, navigate to the Security option, and select the HTTPS entry for the TRANSPORT PROTOCOL option.

4. Finally, you set the WS encryption and digital signature by selecting the Require Signature and Require Encryption entry for inbound requests and the ADD SIGNATURE AND ADD ENCRYPTION entry for outbound responses in the SECURITY option under MESSAGE SECURITY.

12.4.9 Security for Web Services

You can use web services to transfer confidential information. This leads to plain requirements for the security of SOAP messages: data integrity, data confidential-
ity, and authentication of messages (see Chapter 7). Referring to the information provided in the previous section, Table 12.3 lists the OASIS standards that Release 7.1 of SAP NetWeaver PI currently supports.

<table>
<thead>
<tr>
<th>OASIS Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOAP (1.1)</td>
<td>SOAP is a transport protocol for data communication between heterogeneous and distributed systems using XML messages.</td>
</tr>
<tr>
<td>SOAP (1.2)</td>
<td>Version 1.2 of SOAP adds the XML infoset concept to the standard. This concept defines enhancements for the communication format.</td>
</tr>
<tr>
<td>WSDL (1.1)</td>
<td>The Web Services Description Language WSDL is used to describe document-oriented or procedure-oriented XML information, such as SOAP messages or UDDI as part of the Enterprise Services Repository or Services Registry.</td>
</tr>
<tr>
<td>UDDI (3.02)</td>
<td>Information on web services needs to be structured, stored, and managed in an inventory directory to make web services available. Universal Description, Discovery and Integration (UDDI) is the standard for this kind of directory.</td>
</tr>
<tr>
<td>XML (1.0)</td>
<td>Extensible Markup Language (XML) is a programming language to provide information as documents that can also contain instructions for their processing. XML is the basis for all kinds of web service programming.</td>
</tr>
<tr>
<td>HTTP (1.1)</td>
<td>The Hypertext Transfer Protocol (HTTP) is a transfer protocol for information between heterogeneous and distributed systems.</td>
</tr>
<tr>
<td>WS-Policy Attachment (2004/09)</td>
<td>The WS-Policy Attachment defines WS-Policy assertions (WSDL 1.1 Attachments only) that describe a condition, characteristic, or behavior of web services.</td>
</tr>
<tr>
<td>WSIL (1.0)</td>
<td>The Web Service Inspection Language (WSIL) is used to inspect systems that offer web services. This is necessary for user systems of web services to identify appropriate web services.</td>
</tr>
<tr>
<td>WS-Addressing (1.0)</td>
<td>WS-Addressing is used to identify and exchange web services using XML infosets.</td>
</tr>
<tr>
<td>WS-Reliable Messaging (1.1)</td>
<td>WS-Reliable Messaging is a concept for reliable message transfer using web services.</td>
</tr>
<tr>
<td>WS-Security (1.0)</td>
<td>WS-Security is the OASIS framework for web service security. It describes standards for authentication, digital signatures, and encryption of SOAP XML messages.</td>
</tr>
</tbody>
</table>

Table 12.3 OASIS Standards for Web Services in SAP NetWeaver PI
WS-SecurityPolicy (1.2) The WS-SecurityPolicy constitutes the framework of guidelines for web services with regard to their security.

WS-SecureConversation (1.3) WS-SecureConversation is a part of the WS-Policy and provides support for avoiding multiple authentication.

WS-I Basic Profile (1.1) The WS-I Basic Profile supports the interoperability of web services in combination with SOAP, WSDL, and UDDI.

SAML (2.0) The Security Assertion Markup Language (SAML) is the current standard for the description of XML documents. SAML communicates, for example, what information is required for authentication and protection of objects and how X.509 certificates are used as a proof of security. SAP NetWeaver Portal 7.0 supports SAML 2.0.

WS-Security: SAML Token Profile (1.0) An SAML Token Profile contains information on the authentication of objects and is used like an X.509 certificate as a proof of security.

Table 12.3 OASIS Standards for Web Services in SAP NetWeaver PI (Cont.)

For example, if a web service interacts with an AS ABAP (the SAP system can be both in this scenario, service provider and service consumer), this web service must be authorized in the traditional way according to the known ABAP authorization concept. Table 12.4 lists the standard roles available for this purpose.

<table>
<thead>
<tr>
<th>Standard Role (ABAP)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP_BC_WEBSERVICE_SERVICE_USER</td>
<td>Role for background users of the WS runtime</td>
</tr>
<tr>
<td>SAP_BC_WEBSERVICE_ADMIN_TEC</td>
<td>Technical administration of web services, for example, for monitoring or managing communication channels</td>
</tr>
<tr>
<td>SAP_BC_WEBSERVICE_ADMIN_BIZ</td>
<td>Administrator for the administration of the functional use of web services</td>
</tr>
<tr>
<td>SAP_BC_WEBSERVICE_CONSUMER</td>
<td>System user for the use of web services</td>
</tr>
<tr>
<td>SAP_BC_WEBSERVICE_OBSERVER</td>
<td>Read authorization for all web services and for information monitoring</td>
</tr>
<tr>
<td>SAP_BC_WEBSERVICE_DEBUGGER</td>
<td>Authorization for WS debugging (troubleshooting)</td>
</tr>
</tbody>
</table>

Table 12.4 Standard Roles (ABAP) for Web Services in SAP NetWeaver PI 7.1
Index

A

A2A, 355
ABAP, 258
ABAP Workbench, 258
authorization, 462
authorization concept, 269, 279, 533, 622
function group, 283
kernel, 297
program, 564
role, 474
software development, 306
stack, 258, 269
Ability to check
critical authorization, 220
Ability to reproduce, 35
Access control, 214, 333, 395, 555, 600, 601
Access Control Engine, 629, 634, 635
Access control list, 333, 379, 440, 459, 641, 714
Access level, 336
Access permission, 566
Accounting Reform Act, 92
ACS, 163
Active Directory, 429, 451, 487
Active threat, 36
ActiveX control, 705
Activity group, 566
Adapter, 365
Adapter object, 668
Ad hoc query, 326
Ad hoc reports, 310
Administrator Workbench, 314
Advanced analytics, 327
Advanced Encryption Standard, 129
Advanced Planning and Optimization, 641
Advanced rights, 338
AES, 129
AGate, 408, 412
Aggregation
data retention, 310
Alarm
memory problem, 525
ALE, 272
distribution model, 577
Analysis, 223
Analysis authorization, 318
Analysis of objectives, 36
Analysis phase, 66
Analytical data, 309
Anonymous user, 428, 491
Antivirus protection
missing, 708
Antivirus scan
missing, 455
Antivirus scanner, 526
Apache, 494
API, 443
Applicant authorization, 612
Application
authorization, 343
layer, 146
security, 563
Application-level firewall, 297
Application-level gateway, 150, 151, 299, 304, 377, 389, 496, 688
Application Link Enabling -> see ALE, 272
Application process, 226
Application programming interface -> see API, 443
Application security, 70
Approva, 168
AP&RC, 160
Architecture
service-oriented -> see SOA, 175
Architecture landscape, 55
Assignment object, 674
Asymmetric encryption, 129
Asynchronous data storage, 669
Attack
external, 454
Audit, 377
function, 345
message exchange, 389
requirement, 306
Audit Information System, 291, 588
Auditing, 80
Authentication, 51, 171, 484, 563
certificate-based, 412, 419
Kerberos, 420
mechanism, 352, 563
method, 345
missing, 387, 707
mutual, 377, 397
option, 470
procedure, 140
two factors, 142
X.509, 392
Authenticity, 35
AUTHORITY-CHECK, 564
Authorization, 184, 192, 343, 429, 516, 555, 563, 567, 574
assignment, influencing factor, 225
batch processing, 583
check, 307
component, 70, 557, 566, 569
conflict, 338
design, 69, 558, 589
environment, 556
field, 566, 585
functional, 575
group concept, 578
information system, 588
level, 611
main switch, 610
management, 252, 557, 597
missing concept, 447
object, 216
object type, 317
object-typical, 335
organizational, 575
portal role, 459, 635
procedure, 611
profile, 216, 567, 569, 574
query, 584
report, 582
Report Writer and Report Painter, 585
role, 216
SAP Event Management, 643
SAP system, 71
special solution, 319
spool and printer, 585
strategy, 561
structural, 320
systems, 51
table, 578
test, 68
tolerance period, 614
Authorization check, 568
customized, 614
obligatory, 573
optional, 574
relevance, 574
reporting, 613
SAP NetWeaver BW, 314
tolerance period, 610
Authorization concept, 269, 508, 529, 540, 557, 578
comprehensive, 559
example, 339
inadequate, 541, 621, 640, 649
Java application, 277
missing, 351, 384
mobile application, 515
SAP BusinessObjects, 332
technical, 269
Authorization field
RFC_NAME, 534
Authorization object, 564, 566, 585
class, 568
role, 575
SAP NetWeaver BW, 316
S_DEVELOP, 306
S_ICF, 283
S_LOG_COM, 293
S_RFC, 284, 534
S_RFCACL, 285, 644, 666
S_RZL_ADM, 293
Authorization objects, 564
Authorizations
with hierarchy, 320
Available-to-Promise, 643
Avira, 173
Avoidance, 79
Awareness for security, 714
missing, 710
### Index

**B**

<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>B2B, 355</td>
<td></td>
</tr>
<tr>
<td>Backdoor option, 497</td>
<td></td>
</tr>
<tr>
<td>Background job, 583</td>
<td></td>
</tr>
<tr>
<td>Backup concept, 714</td>
<td></td>
</tr>
<tr>
<td>missing, 680, 709</td>
<td></td>
</tr>
<tr>
<td>Backup copy, 602</td>
<td></td>
</tr>
<tr>
<td>Balanced scorecard, 619</td>
<td></td>
</tr>
<tr>
<td>Banking Act, 95</td>
<td></td>
</tr>
<tr>
<td>Banking control area, 94</td>
<td></td>
</tr>
<tr>
<td>BAPI, 175, 186, 257, 477</td>
<td></td>
</tr>
<tr>
<td>Barcode, 527</td>
<td></td>
</tr>
<tr>
<td>Basel, 94</td>
<td></td>
</tr>
<tr>
<td>Basel II, 95</td>
<td></td>
</tr>
<tr>
<td>Baseline, 541</td>
<td></td>
</tr>
<tr>
<td>Baseline protection, 120</td>
<td></td>
</tr>
<tr>
<td>Batch processing</td>
<td></td>
</tr>
<tr>
<td>authorization, 583</td>
<td></td>
</tr>
<tr>
<td>BDSG, 115, 599</td>
<td></td>
</tr>
<tr>
<td>Best Practice, 59, 589</td>
<td></td>
</tr>
<tr>
<td>Best-practice method</td>
<td></td>
</tr>
<tr>
<td>analysis of objectives, 36</td>
<td></td>
</tr>
<tr>
<td>best-practice analysis, 59</td>
<td></td>
</tr>
<tr>
<td>control analysis, 46</td>
<td></td>
</tr>
<tr>
<td>danger analysis, 44</td>
<td></td>
</tr>
<tr>
<td>four-eyes principle, 100</td>
<td></td>
</tr>
<tr>
<td>highly integrated and holistic solution, 97</td>
<td></td>
</tr>
<tr>
<td>impact analysis, 45</td>
<td></td>
</tr>
<tr>
<td>information ownership, 87</td>
<td></td>
</tr>
<tr>
<td>integrated, holistic solution, 88, 92</td>
<td></td>
</tr>
<tr>
<td>interaction of the organizational structure, 77</td>
<td></td>
</tr>
<tr>
<td>method concept, 58</td>
<td></td>
</tr>
<tr>
<td>monitoring and reporting, 86</td>
<td></td>
</tr>
<tr>
<td>protection requirements analysis, 40</td>
<td></td>
</tr>
<tr>
<td>requirements analysis, 57, 80</td>
<td></td>
</tr>
<tr>
<td>risk analysis, 41</td>
<td></td>
</tr>
<tr>
<td>risk control analysis, 48</td>
<td></td>
</tr>
<tr>
<td>security phase, 66</td>
<td></td>
</tr>
<tr>
<td>segregation of duties, 99</td>
<td></td>
</tr>
<tr>
<td>strategy concept, 58</td>
<td></td>
</tr>
<tr>
<td>BEx, 316</td>
<td></td>
</tr>
<tr>
<td>Web, 316</td>
<td></td>
</tr>
<tr>
<td>BEx Analyzer, 316</td>
<td></td>
</tr>
<tr>
<td>BEx Query Designer, 316</td>
<td></td>
</tr>
<tr>
<td>Biometric fingerprint, 143, 713</td>
<td></td>
</tr>
<tr>
<td>Biometric identification, 563</td>
<td></td>
</tr>
<tr>
<td>BM, 162</td>
<td></td>
</tr>
<tr>
<td>BPR, 161</td>
<td></td>
</tr>
<tr>
<td>BPS, 163</td>
<td></td>
</tr>
<tr>
<td>British Standards Institution, 102</td>
<td></td>
</tr>
<tr>
<td>Brute-force attack, 511, 522</td>
<td></td>
</tr>
<tr>
<td>BSI, 101</td>
<td></td>
</tr>
<tr>
<td>BSP, 257, 267, 301, 392, 410</td>
<td></td>
</tr>
<tr>
<td>Buffer overflow, 151, 267, 454, 497</td>
<td></td>
</tr>
<tr>
<td>Business consolidation, 619</td>
<td></td>
</tr>
<tr>
<td>Business Explorer -&gt; see BEx, 316</td>
<td></td>
</tr>
<tr>
<td>Business Intelligence, 309</td>
<td></td>
</tr>
<tr>
<td>Business partner, 53</td>
<td></td>
</tr>
<tr>
<td>Business planning and simulation, 619</td>
<td></td>
</tr>
<tr>
<td>Business process, 49, 53</td>
<td></td>
</tr>
<tr>
<td>Business-relevant master data, 427</td>
<td></td>
</tr>
<tr>
<td>Business Server Page -&gt; see BSP, 257</td>
<td></td>
</tr>
</tbody>
</table>

**C**

<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caesar code, 128</td>
<td></td>
</tr>
<tr>
<td>Canonicalization, 526</td>
<td></td>
</tr>
<tr>
<td>Central information system, 309</td>
<td></td>
</tr>
<tr>
<td>Central Management Console, 326, 333</td>
<td></td>
</tr>
<tr>
<td>Central User Administration, 77, 275, 429, 606</td>
<td></td>
</tr>
<tr>
<td>Certificate, 486</td>
<td></td>
</tr>
<tr>
<td>digital, 137, 143, 563, 699</td>
<td></td>
</tr>
<tr>
<td>person-related, 489</td>
<td></td>
</tr>
<tr>
<td>Certificate authority, 138, 288, 363, 693</td>
<td></td>
</tr>
<tr>
<td>TrustedCA, 372, 374</td>
<td></td>
</tr>
<tr>
<td>Certificate Authority (CA), 127</td>
<td></td>
</tr>
<tr>
<td>Certificate-based authentication, 412, 419</td>
<td></td>
</tr>
<tr>
<td>Certificate revocation list, 133, 697</td>
<td></td>
</tr>
<tr>
<td>Certificate signing request, 301</td>
<td></td>
</tr>
<tr>
<td>Certificate storage location, 301</td>
<td></td>
</tr>
<tr>
<td>Certification, 103</td>
<td></td>
</tr>
<tr>
<td>CGI program, 398</td>
<td></td>
</tr>
<tr>
<td>Challenge-response procedure, 140</td>
<td></td>
</tr>
<tr>
<td>Change management, 70, 305, 480, 559</td>
<td></td>
</tr>
<tr>
<td>Check, 223</td>
<td></td>
</tr>
<tr>
<td>Check for Revocation, 706</td>
<td></td>
</tr>
<tr>
<td>Check indicator, 572, 574</td>
<td></td>
</tr>
<tr>
<td>type, 574</td>
<td></td>
</tr>
</tbody>
</table>
Index

Chemical
management, 251

safety, 250

Chemical substance, 98

CIDX, 372

Classification, 241
information asset, 104

Client, 291

Cluster, 259, 610

CM&SC, 160

CobiT, 101, 107
acquire and implement, 108
domain, 108
maturity model of internal controls, 107
monitor and evaluate, 108
plan and organize, 108
security baseline, 109

CoBIT, 107

Collaboration, 439
agreement, 350

Communication
unencrypted, 265

Communication channel, 33
encrypted, 500
unencrypted, 531

Communication connection, 428, 542
encrypted, 535

Communication partner
interaction, 195

Communication security, 527

Company asset, 35, 36, 42
classification, 39
indirect, 39
physical and informational, 38

Company assets, 51

Company culture, 248

Company objective, 36

Complexity criteria, 683

Complex password, 353

Compliance, 35, 106, 203, 238, 325
analysis, 80
management, 241, 242, 250, 253
risk, 54
structure, 233

Compliant User Provisioning, 225

Component worth protecting, 37

Composite role, 567, 571

Comprehensive authorization concept, 559

Computer Associates, 170, 172

Computer Security Institute, 88

Computing Center Management System, 379, 390, 524, 551

Configuration control, 204

Connection port
open, 709

Connector, 347, 383

Connector Framework, 442

Continuity phase, 66

Control, 45, 112, 210, 587
classification, 46
downstream, 46
element, 216
evaluation, 89
instrument, 220
internal, 71
legal, 241
management, 117
operating, 118
preventive, 589
technical, 118
type, 45
upstream, 46

Control analysis, 46, 62

Control measure, 51

Controls, 72

Control solution
Evaluation, 556

Control system, 79

Control table, 616

Cookie, 344
manipulation, 526
poisoning, 267, 392, 454, 496
web browser, 288

CORBA
service, 346
technology, 331

Corporate governance, 51, 54, 81, 197
proper, 203

Corporate Performance Management, 619

COSO, 101, 112
enterprise risk management framework, 112
Index

CPC, 162
CPI-C
  application, 264
  protocol, 291
CPP, 162
Credit risk, 95
Cross-site scripting, 151, 267, 392, 454, 497, 526
Cryptography, 127
  asymmetric encryption, 127
  elliptic curve cryptography, 130
  hybrid encryption procedure, 131
  modulo function, 130
  pair of keys, 129
  plain text, 130
  private key, 129
  public key, 129
  session key, 131
Crystal Reports, 333
CSL, 162
CUA, 77, 275, 429, 577, 606
Custom development, 269
  gaps, 514
Customer data, 626
Customs, 239
  procedure, 243
Customs Management, 243

D
Damage claim, 253
Danger, 37
  analysis, 44
Danger analysis, 62
Dashboard, 211, 326
Data
  encryption, 127, 601
  insufficient security, 621
  manipulation, 531
  master data, 423
  modification, 267
  object, 309
  personal, 602
  presentation, 310
  quality, 239
  query, 314
  retention, 310
  security, 600, 686
  structured and unstructured, 309
  theft, 267
  transactional and analytical, 309
  transaction data, 423
  unencrypted transfer, 455
Database
  limit access, 686
  remove users, 686
  unauthorized query, 680
  unprotected, 679
  user entry, 679
Database server, 677
  application security, 681
  risk and control, 678
  technical security, 683
  upgrade concept, 688
Data Encryption Standard, 129, 191
Data link layer, 148
Data on demand, 706
Data Orchestration Engine, 519
Data protection, 35, 599
  guide, 602
  Human Resources, 599
  inadequate, 640, 650
  law, 425
  legal requirement, 599
  official, 600
Data protection law, 115
Data security, 540
Data source
  configuration file, 444, 489
Data storage
  asynchronous, 669
Data warehouse management, 314
DB2, 681
  database user, 684
DDIC, 263, 291
Deactivation, 301
  service, 511
Debug option, 497
Decision-maker, 201
Default password, 291, 305
  change, 291, 683
Index

Default port, 686
Default user, 263
Defense in depth, 145
Defense-relevant process, 669
Definition file, 502
Delegated user administration, 472
Delegation, 238
Deliver and support, 108
Delta link, 459
Demilitarized zone -> see DMZ, 396
Denial of service, 401
Deny All, 172
Deployment Descriptor, 278, 279
DER format, 486
Derivation role, 575
Design, 67
Design phase, 66
Design role, 566
Design Time Repository, 307
Determination
legal, 57
Device
mobile, 167, 506, 669
Digital certificate, 137, 143, 563, 699
Digital signature, 135, 183, 380, 389, 526
document, 697
for XML message, 371
Directory service, 78
Directory traversal, 151, 526
Disclosure control, 601
Dispatcher, 690
Distinguished name, 299, 482
Division of duties, 105
DMZ, 396, 401, 411, 493, 636
collection, 523
Documentation, 59
document format
electronic, 694
Downstream control, 46
DPP, 162
Drilldown, 314
Dual-host configuration, 409
Dynamic Information and Action Gateway, 265, 297, 404, 408, 690

E

EAI, 347
EarlyWatch, 291
eCATT, 274
Economic model, 50
ECR, 160
EERM, 253
EFR, 160
EIR, 161
EJB, 278
Electronic Compliance Reporting, 247
Electronic Data Interchange, 241
Electronic document format, 694
Emergency
authorization, 228
collection, 602
Emission management, 253
Employee Self-Service, 612
EMR, 160
Encryption, 380, 389
generator, 183
asymmetric, 129
communication, 380, 500, 535
hybrid, 131
symmetric, 128
Encryption mechanisms, 51, 713
Energy efficiency, 255
ENR, 161
Enterprise Application Integration -> see
EAI, 347
Enterprise Environmental Risk Management, 253
Enterprise financial and commercial risk, 208
Enterprise JavaBean, 278
Enterprise risk management, 49, 50, 197, 205, 212, 238, 239
strategy, 49, 53, 57
Enterprise Role Management, 227
Enterprise service, 175, 187
security, 190
Enterprise Service Bus, 347
Enterprise Services Builder, 348, 351, 357
audit, 377
authorization, 357
change history, 378
Enterprise Services Repository, 348, 351
Enterprise Services Workplace, 187
Enterprise software, 33
Entrust, 170, 172
Environment, 252
specification, 250
Environmental compliance risk, 208
Environmental protection, 248
Environmental risk, 253
Environmental specification, 254
product-related, 252
ERM Navigation Control Map, 155
Error message, 401
ETR, 161
Evaluation, 66
control solution, 556
individual, 211
Evaluation setup, 234
Export license, 239
Extensible Access Control Markup Language, 182
External attacks, 454

F

F5 TrafficShield, 172
FB50, 113, 456
FBI, 88
FBV0, 113, 456
FDA, 93
Federal Bureau of Investigation, 88
Federal Data Protection Act, 599
Federal Office for Information Security, 101
Field group
authorization concept, 582
concept, 581
File, 383
File adapter
secure, 390
securing, 379
Financial process, 49
Financial reporting, 80
Fingerprint
biometric, 713
Firewall, 51, 150, 266, 377, 703
personal firewall, 704, 714
Flow control, 149
Forceful browsing, 497
Foreign trade, 238, 239
Four-eyes principle, 100, 261, 415, 456
FTP, 347, 383
Function access, 226
Functional authorization, 575
Function role, 571

G

General framework, 56
Generic Security API, 699
Generic user, 428
German Commercial Law, 92
German Electronic Signature Act, 698
Globalization, 49
Goal definition phase, 207
GoB, 90
GoBS, 90
content, 90
Good practice -> see Best Practice, 59
Governance, 182, 203
Governance, Risk, and Compliance, 180, 197
GPRS, 508
GRC solution
deployment planning, 200
goal, 198
method, 199
GRMG, 525
Group
caption, 334
hierarchy, 334
GSM, 508
Guest account, 305
Guest user, 296, 342
Guidelines, 57
Handshaking, 133
Hardware Security Module, 140
Hash procedure, 134
Hash value, 522
Hazardous goods management, 251
Health, 252
Health protection, 248
Heartbeat, 524
Hidden field, 496
Hierarchical authorizations, 320
Hierarchy, 482
Highly integrated solution, 97
High-security environments, 672
Holistic solution, 88, 92, 97
HR data, 290, 602
HRR, 161
HSM, 140
HSR, 162
HTTP, 297, 437, 702
HTTP(S), 260, 389, 394, 417, 532, 535
response, 497
Human Capital Management -> see SAP ERP HCM, 599
Human resources security, 104
Hybrid encryption, 131
Hyperlink, 333
Hypertext Transfer Protocol -> see HTTP, 702

IA&BL, 162
IAIK
security package, 363
IBM Tivoli, 171
ICF, 265, 301, 397, 410
ICM, 258, 301, 396, 523
ICS, 91
IDEA, 129
Identification
biometric, 563
Identities, 74
Identity, 54
Identity management, 74, 76, 77, 427, 429, 605
solution, 77
Identity theft, 605
ID mapping, 432, 433
IDoc, 175
IDS, 146, 268, 305
IFRS, 92
IM, 162
Impact analysis, 45, 62
Impact scorecard, 208
Implementation, 68
Implementation phase, 66
Improvement phase, 66
Inadequate authorization concept, 621, 640, 649
Inadequate data protection, 640, 650
Inconsistent master data, 427
Indirect company asset, 39
Indirect role assignment, 615
Indirect user assignment, 675
Individual analysis, 47
Individual evaluation, 211
Industry-specific requirement, 93
Industry-specific risk, 42
Influencing component, 36
Influencing factor, 75
proper authorization assignment, 225
InfoAreas, 314
InfoCube, 309, 314, 316
InfoObject, 314, 316
administration, 318
Informational company asset, 38
Information asset
classification, 104
Information Broadcasting, 323
Information ownership, 68, 87, 104, 472, 473, 479
principle, 558, 589
Information responsibility, 533
Information Security Management System, 103
Information system
central, 309
Information technology risk, 208
Infotype, 610
Index

Infrastructure
  technical, 55
Inheritance, 338
Inheritance principle, 575
Input control, 601
Inspection, 614
Integrated ITS, 407, 421
Integrated solution, 88, 92
Integration
  agreement, 350
  scenario, 376
  test, 68
Integration Builder, 358
Integration Directory, 351
Integration Server, 349, 383
Integrity, 35
Interface -> see API, 443
Internal control, 71, 91
Internal requirement, 57, 99
International Data Encryption Algorithm, 129
International Financial Reporting Standards, 92
Internet Communication Framework, 265, 301, 397, 410
Internet Communication Manager, 258, 301, 396, 523
Intrusion detection system, 146, 268, 305
IP address, 405
IPF, 253
iPPE
  authorization profile, 642
  Workbench, 642
IRR, 162
Irrevocability, 181
ISMS, 103
ISO, 102
ISO/IEC, 101, 103, 110
ISR, 162
IT application, 50
IT department, 557
ITGI, 107
IT Governance Institute, 107
IT-Grundschutz catalog, 101, 120
  component, 120
ITIL, 101, 110, 539
  process, 539
IT Infrastructure Library -> see ITIL, 110, 539
ITR, 161
IT security, 51, 127
  core objective, 35
  description, 35
  objective, 35
  strategy, 36
IT systems, 56
iView, 441, 443, 453, 458
  authorization check, 470
J
  J2EE config tool, 465
  J2EE dispatcher, 299
  J2EE Engine, 257, 275
  JAAS, 277, 421
  authorization concept, 278
  Jasper log function, 523
  Java
    role, 388
  Java Connection Architecture, 442
  Java Connector
    connection, 520
  Java Deployment Descriptor, 279
  JavaServer Page, 257, 267, 277, 288
  Java SSF Library, 696
  JDBC, 298, 383
  JEE5, 347
  JMS, 383
  Job monitor, 234
  J-SOX, 89
  JSP, 257, 267, 277, 288
K
  KDC, 141
  Kerberos, 141, 182
  authentication, 288, 420, 487
  SPNEGO, 699
  token, 182
Key distribution center, 141
Key risk, 207
Key Risk Indicator, 207
Key storage provider, 372
Keystore, 301
    service, 486
Knowledge management, 440, 442
KWG, 95

L
Launch pad, 221
LDAP, 290, 297, 429, 444, 482, 606
    directory, 263, 290
    directory service, 77
    server, 491
Legal compliance, 197, 203
Legal control, 241
Legal determination, 57
Legally binding nature, 35
Legal requirement, 79
Legal risk, 42, 54
Level of confidentiality, 39
Liability risk, 253
Load balancing, 392
Logging, 601
Logon token, 344, 346
Long-term archiving, 687

M
Magnetic card, 563
Mail, 383
Malware, 702
Management
    control, 117
Management cockpit, 619
Management of Internal Controls, 223
Market discipline, 95
Market risk, 206, 208
Mass change, 577
Master data, 241, 423
    authorization, 610
    business-relevant, 427
    inconsistent, 427
    management, 432
    person-related, 425
Master Data Client, 436
Master Data Server, 433
Material group, 241
MD5, 134
Memory problem
    alarm, 525
Menu, 574
Message Digest Algorithm 5, 134
Message exchange
    audit, 389
Message security, 374, 379
Metadata repository, 310
Method
    concept, 58
MIC, 161, 223
Microsoft Windows
    Active Directory, 451, 487
    authentication, 685
    NTLM, 699
    Trust, 488
Middleware, 357, 360, 391
MiniApp, 516
Minimum capital requirements, 95
Minimum requirement for regulation, 602
Misconfigured portal, 452
Missing antivirus protection, 708
Missing antivirus scan, 455
Missing authentication, 387, 707
Missing authorization concept, 351, 384, 447
Missing awareness for security, 710
Missing backup concept, 680, 709
Missing monitoring concept, 512
Missing network segmentation, 511
Missing network strategy, 453
Missing signature, 386
Missing upgrade concept, 681
MM01, 457, 565
Mobile client, 506
Mobile Component Descriptor, 515
Mobile device, 167, 506, 669, 706
    application security, 712
    authentication, 712
    risk and control, 707
    technical security, 712
Mobile scanner, 505
Model
  economic, 50
Module, 555
Monitoring, 86, 211, 237, 403, 537, 587
  scheduler, 234
Monitoring tool, 389
Multiple-user concept, 707
Mutual authentication, 396

NAFTA, 238
Naming
  convention, 594
Narcotics law, 242
National Institute of Standards and Technology, 101, 117, 129
Need for security, 34
Network architecture
  secure, 303, 493, 535
Network communication, 346
Network interface protocol, 149
Network layer, 148
Network segment, 677
Network segmentation, 411, 415
  missing, 511
Network strategy
  missing, 453
NIST, 101, 117, 129
North American Free Trade Agreement, 238
Novell eDirectory, 171
NTLM, 699
NWDS, 506

OASIS, 177, 183
  consortium, 177
  standard, 179, 188, 192
Objective analysis, 61
Object type
  group, 336
Object-typical authorization, 335
Obligatory authorization check, 573
OCR, 161
OC&RM, 160
OCSP, 697
OLAP, 323
OLTP, 323
One-factor authentication
  Single Sign-On, 484
One-factor procedure, 140
Online Certificate Status Protocol, 697
Open connection port, 709
Operating control, 118
Operating system, 304
  command, 264
Operating system access
  restriction, 293
Optional authorization check, 574
Oracle, 170, 682
  database user, 684, 685
Organizational and change management risk, 208
Organizational authorization, 575
Organizational hierarchy, 613
Organizational key, 612
Organizational level, 575
Organizational risk, 43
Organizational structure, 77
Organizational unit
  as control element, 565
Organization for the Advancement of Structured Information Standard, 177
OSI, 395
OSI model, 127, 678
  application layer, 180
  layer, 144, 145
OVA7, 578

Package filter, stateful, 150
Parameter tampering, 151, 496
PAS, 420
  module, 421
Passive threat, 36
Passphrase, 142
Index

Password, 262, 352, 412
  06071992, 291
  19920706, 291
authentication, 552, 644, 665
change, 291, 678, 683
complexity, 291, 353, 683
default password, 263, 291, 305, 683
hard disk, 601
length, 522
quality, 450, 451
rule, 264, 296, 342, 361, 534, 560
security, 526
synchronization, 523
too simple, 531
Patching, 688
PCAOB, 81
PCD, 441, 458, 462
People-Centric UI, 432
Permission Editor, 469
Persistence Manager, 444
Persistence storage, 444
Personal data, 602
Personal digital assistant, 713
Personal firewall, 704, 714
Personal Information Protection and Electronic Documents Act ->, 122
Personal Security Environment, 289, 299, 364, 400, 417, 418, 419
Personnel development, 614
Personnel number check, 612
Personnel planning authorization, 613
Person-related certificate, 489
Person-related master data, 425
PFCG, 440, 457, 478, 516, 566, 572
PFUD, 577
P&GP, 160
Pharmaceutical law, 242
Physical assets, 38
Physical company asset, 38
Physical layer, 149
Physical security, 105
Pilot test, 68
PIPEDA, 101, 122
data protection principle, 123
personal data, 123
PKI, 127, 130, 137, 412, 491, 693
certificate revocation list, 133, 139
Plain text, 331
Planning phase, 66, 208
Pluggable Authentication Service -> see PAS, 420
Plug-in
  security, 345
Point of control, 564
Policy alternative, 183
Policy assertion, 183
Political risk, 206
Portal content directory, 458
Portal role, 430
  authorization, 459, 635
  concept, 282
  structure, 457
Poster -> see ERM Navigation Control Map, 155
Potential risk, 211
  influencing parameter, 40
Power users, 322
PPOCA_BBP, 660
PPOMA_BBP, 660
Presentation layer, 146
Preventive control, 589
Principal, 278, 334, 340, 342
  security, 337
Principle, 59
  information ownership, 558
Principle of information ownership, 68
Principles for Accounting, 90
Principles of Computer-Based Bookkeeping, 90
Procedure
  biometric, 143
Process
  control, 229
defense-relevant, 669
  risk, 42
Process-related risk management, 203
Product
  classification, 242
  safety, 251
Production phase, 66
Product-related environmental specification, 252
Profile concept, 334
Program code, 269, 514
Proper corporate governance, 203
Protection need, 39
Protection requirement, 556
Protective factor, 211
PSE, 289, 299, 364, 400, 417, 418, 419
PSR, 161
Public Company Accounting Oversight Board, 81
Publicity control system, 82
Public key certificate, 290
Public key infrastructure-> see PKI, 127, 412

Q

Quality assurance, 305
process, 268, 305, 688
Query
authorization, 584
component authorization, 316
template, 316
QuickView, 584

R

Radio Frequency Identification -> see RFID, 527
RAR, 222
Rating, 95
REACH, 98
Receiver agreement, 350, 373
Reference model, 89
Reference role, 674
Registration authority, 138
Release process, 235
Release workflow, 660
Relevance
authorization check, 574
Reliability, 35
Remote user, 432
Replication Manager, 447
Report
RSUSR300, 418
RSUSREXTID, 420, 422
Report center, 236
Reporting, 70, 86, 214
environment reporting, 254
Reporting object, 316
Requirement, 79, 93
analysis, 57, 80
catalog, 57
industry-specific, 93
internal, 57, 99
legal, 79
legal data protection, 599
Requirements, 56
Requirements catalog, 61
Responsibilities, 73
Responsibility, 87, 212
Responsibility structure, 557
Restriction
operating system access, 293
Return on Environmental Investment, 254
Return on security investment, 81
Return on Security Investment Planning, 201
Reverse proxy, 297, 304, 389, 392, 395, 494
authorization, 261, 283
call, 283, 285
communication, 351, 429, 551, 644
destination, 292
object, 284
security environment, 665
system user, 429
trusted RFC connection, 665
user, 261, 283, 519, 534, 552
RFCDES, 284, 292
RFC_NAME, 534
RFID, 505, 527
device, 533
Rights assignment
stepwise, 225
Risk, 34, 37, 40
analysis, 41, 456, 535, 540
area, 209
classification, 44
control, 197

733
Index

definition, 52
environmental risk, 253
group, 209
key risk, 207
legal and industry-specific, 42
management, 257
market risk, 206
organizational, 43
planning, 207
political, 206
potential, 34, 556
process risk, 42
relevance, 271
risk of loss, 41
technical, 42
type, 41, 43
Risk analysis, 62
Risk Analysis and Remediation, 222
Risk and control management, 33, 41
Risk control analysis, 45, 47, 48, 61, 62
Risk control system, 198, 211
Risk management, 96, 203
authorization role, 213
component, 207
organization, 212
process, 207, 214
process-related, 203
project, 208
strategy, 208
user role, 212
Risk of loss, 41
Risks, 62
RM, 162
RMS, 162
RNIF, 372
RoEI, 254
RoHS, 252
Role, 272, 429, 567, 574
assignments, 238, 615
attribute, 227
category, 571
change, 675
concept, 563, 570
derived, 576
JAAS, 278
menu, 574
module, 227
reference role, 674
type, 571
Role Assigner, 461, 473
Roles, 70, 566
Root folder
security, 335
RosettaNet, 347
RoSIP, 201
RSA, 191
RSA Access Manager, 172
RSA algorithm, 129
RSD, 163
RSD1, 318
RSECADMIN, 318, 319
RSSM, 316
RSUSR300, 418
RSUSREXTID, 420, 422
Rules-based security check, 659
RZ20, 524

S

SA38, 582
Safety, 252
chemical, 250
product, 251
Safety level, 467
SAML, 143, 182, 377
Sanction list check, 241
SAP
Authorization System, 214
default role, 432
Environmental Compliance, 254
middleware, 391
Risk Management, 197
security concept, 64, 589
solution for internal and external
security, 668
system availability, 305
SAP*, 263, 291
SAP Active Global Support, 672
SAP_ALL, 261, 519, 530, 534, 640, 650
SAP Audit Information System, 168
SAP Auto-ID Infrastructure, 166, 527
application security, 533
authorization concept, 533
authorization object, 534
risk and control, 529
standard role, 533
technical security, 535
SAP BusinessObjects, 161, 325
Access Control, 214, 220
application security, 332
authorization concept, 332
BI solution, 325
deployment planning of GRC, 200
Global Trade Services, 238
GRC component, 198
GRC goal, 198
GRC method, 199
GRC solution, 197, 479
launch pad, 221
password rule, 342
Process Control, 202, 229, 231
repository, 199
risk and control, 327
Risk Management, 202, 209
Sustainability Performance Management, 255
technical security, 344
user concept, 333
SAP Content Integrator, 428, 430, 434
SAP CRM, 163, 625
Access Control Engine, 629
application security, 628
backend system, 628
risk and control, 626
server, 628
technical security, 636
SAP Cryptographic Library, 299, 363, 417, 695
SAPCRYPTOLIB, 299, 363, 417, 695
SAP Enterprise Buyer, 651, 657
SAP Environment, Health, and Safety Management, 248
SAP ERP, 555, 556
application security, 563
risk and control, 556
technical security, 597
SAP ERP Financials, 254, 555
SAP ERP HCM, 69, 77, 483, 555, 599
applicant authorization, 612
application security, 609
main authorization switch, 610
master data authorization, 610
organizational structure, 606
personnel planning authorization, 613
risk and control, 602
structural authorization, 613
structure, 673
technical security, 617
SAP ERP Operations, 555
SAP Event Management, 643
SAP for Defense and Security, 668
SAP Gateway, 264, 291, 293, 436, 551
SAP GUI, 167, 287, 375, 408, 535, 623, 689
application security, 693
risk and control, 690
technical security, 698
variant, 689
SAP industry solution, 667
application security, 671
risk and control, 668
technical security, 675
SAP Internet Transaction Server, 407, 421
AGate, 408
application security, 413
DMZ network segmentation, 415
encryption of communication connections, 417
integrated, 407, 421
risk and control, 410
technical architecture, 408
technical security, 415
WGate, 408
SAP Java Connector, 258
SAP logon ticket, 171, 288, 421, 422, 440, 455, 470, 484, 523, 550
SAP Logon Ticket, 535
SAP MaxSecure, 671, 672
SAP NetWeaver, 165
SAP NetWeaver Application Server, 165, 257, 541
ABAP, 283, 429
application security, 269
Java, 258, 347, 428
risks and control, 260
technical security, 287
Index

SAP NetWeaver Business Warehouse, 69, 309, 325
  application security, 313
  authorization, 314
  authorization check, 314
  authorization element, 314
  authorization object, 316
  authorization pyramid, 315
  risk and control, 310
  technical security, 323
  user, 322
SAP NetWeaver Composition Environment, 307
SAP NetWeaver Developer Studio, 307, 506
SAP NetWeaver Development Infrastructure, 506
SAP NetWeaver Identity Management, 78, 169, 263, 275, 444, 606, 663
SAP NetWeaver Master Data Management, 166, 423
  application security, 429
  Customizing, 432
  identity management, 429
  revision security, 436
  risk and control, 424
  role, 430
  technical security, 436
SAP NetWeaver Mobile, 166, 304, 505, 527, 712
  application security, 515
  authorization concept, 515
  authorization object, 516, 519
  monitoring, 524
  offline scenario, 506
  online scenario, 506
  risk and control, 508
  secure network architecture, 523
  technical security, 520
  Web Console, 518
SAP NetWeaver Portal, 281, 287, 429, 439
  application security, 491
  anonymous access, 491
  application-level gateway, 496
  application security, 496
  approval process, 449
  change management, 480
  connecting LDAP server, 483
  connecting to an SAP system, 483
  database, 444
  technical security, 481
SAP NetWeaver Process Integration, 165, 178, 304, 347, 355, 383, 432
  application security, 357
  encrypt channels, 363
  Integration Server, 383
  risks and control, 350
  technical architecture, 348
  technical security, 361
SAP Partner Connectivity Kit, 377, 383
  application security, 388
  risk and control, 384
  technical security, 389
SAP PLM, 164, 248, 254
SAP Profile Generator, 68, 217, 566, 572, 674
SAP Role Manager, 672
SAProuter, 167, 403, 404, 701
  application security, 405
  network configuration, 406
  risk and control, 404
  string, 407
  technical security, 405
SAP SCM, 164, 254, 528, 639
  application security, 641
  iPPE Workbench, 642
  risk and control, 640
  technical security, 644, 645
SAPSECULIB, 695
SAP SEM, 619
  application security, 622
  risk and control, 620
  technical security, 623
SAP Solution Manager, 260, 537
  application security, 544
  authorization object, 546
Index

functional area, 540
risk and control, 540
technical security, 550, 551
user access, 543
SAP SRM, 164, 647
application security, 651
authorization control, 651
authorization object, 652, 653
business scenario, 648
risk and control, 649
rules-based security check, 659
technical security, 664
user management, 663
SAP system, 540
no monitoring, 541
SAP Web Dispatcher, 167, 391, 494, 636
application security, 395
as a reverse proxy, 395
as a URL filter, 397
risk and control, 392
technical security, 395
Sarbanes-Oxley Act -> see SOX, 80
SAS, 163
SCC4, 306
SC&M, 160
Scoring, 95
Script injection, 498
SCS, 163
SCUA, 577
SCUG, 577
SCUM, 577
S_DEVELOP, 306
SDS, 162
SE03, 306
SE06, 306
SE16, 578
SE38, 582
SE43, 575
SE93, 564, 582
SEC, 81
Secure
file adapter, 390
Secure Hash Algorithm, 134
Secure network architecture, 303, 493, 523, 535
Secure Network Communication -> see SNC, 137, 296, 363, 404
Secure program code, 525
Secure Socket Layer -> see SSL, 296
Secure Storage and Forward -> see SSF, 137
Secure token, 142
SecurID method, 142
Securinfo, 168
Security
calendar, 55
configuration, 291
definition, 34
document, 192
delivery, 153
design, 195
draft, 192
environment, 190
evaluation, 195
framework, 190
function, 192
guideline, 106
human resources, 104
IT, 127
measure, 34
objective, 34
phase, 65, 66
physical, 105
risk, 304, 308
solution, 38
standard, 101, 191
web service, 181, 186
Security and Exchange Commission, 81
Security Assertion Markup Language, 143, 182, 377
Security audit log, 275, 286
Security information log, 588
Security measure, 51
Security plug-in, 345
Security query, 661, 662
Security strategy, 49, 52, 60, 64
procedure, 60
Security zone, 461, 467, 469
Segregation of duties, 91, 99, 113, 456, 472, 473, 479, 545, 558, 575, 602
risk, 217
Sender agreement, 350, 375
SER, 161
Server signature, 694
Service
registration, 195
structure, 195
superfluous, 532
Service-Oriented Architecture -> see SOA, 175
Services Registry, 352
Service user, 362, 385
password, 359
Session layer, 147
Session recording, 672
SHA, 134
Shadow session, 672
S_ICF, 283
SICF, 301, 397, 523
Siemens DirX, 170
Signature, 693
  Control, 697
digital, 135, 389, 526, 697
missing, 386
Sign-off
  status, 235
Simulation function, 620
Single host
  configuration, 409
Single role, 567
  one-factor authentication, 484
  process, 413
Single source of truth, 482
SLD, 349
S_LOG_COM, 293
SM30, 306, 418, 420, 422, 486
SM31, 306, 578
SM36, 525
SM49, 293
SM59, 283, 364
SM69, 293
Smart card, 137, 697
Smart synchronization, 714
SMICM, 363
S/MIME, 372
SMTP, 260
SNC, 137, 265, 296, 375, 363, 404, 417, 500, 508, 535, 552, 623
  communication, 299
  system parameter, 300
SNC_SYSACL, 418
SOA, 33, 175, 176
  concept, 177
governance, 193
  infrastructure, 195
SOAP, 260, 347, 354, 552
  envelope, 177
  header, 177, 372, 377
  message, 179, 191, 380
SoD, 341
Software
  malware, 702
Solution
  integrated and holistic, 88, 92, 97
SOX, 80, 103, 116, 479
  implementation in Japan, 89
  measure, 83, 84, 85
  regulations, 81
SP01, 586
SP02, 586
SPNEGO, 487, 699
Spool request, 584
SP&P, 160
SQ01, 584
SQ02, 584
SQ03, 584
SQL, 687
  injection, 151, 267, 498, 526, 687
  Server, 685
SQVI, 584
S_RFC, 284, 534
S_RFCACL, 285, 644
S_RZL_ADM, 293
SSF, 137, 526
  SSF_Sign, 696
SSH, 131
SSL, 131, 265, 296, 393, 437, 489, 500, 507, 552, 623
  communication, 396
S_TABU_DIS, 306
Staging, 436
Standard authorization, 336, 344
Standard security zone, 469
Standard user, 342
  group, 340
Stealth commanding, 151, 267, 454, 498
Stepwise rights assignment, 225
STMS, 306
Strategy, 57, 64
  concept, 58
  document, 57, 64
Structural authorization, 320, 613
Structured data, 309
STRUST, 289, 363, 364, 400, 418, 486
STRUTSSSO2, 486
SU10, 577
SU24, 572
SU53, 565
SUIM, 113
Superfluous service, 532
Superuser Privilege Management, 228
Supervisory agency, 96
Supervisory review, 95
Supply chain, 639
Supply Chain Planning, 642
Sustainability, 254, 255
SXMB_ADM, 378
SXMB_MONI, 378, 379
Symmetric encryption, 128
Synchronization communication, 521
Synchronization mechanism, 712
synchronization password, 523
SYSADM, 356
System
  integrity, 264
  parameter, 294
System administration, 247
System Landscape Directory, 260, 349

T

T000, 306
T77SO, 610, 614
T77UA, 613
Table
  authorization system, 579
  log, 588
RFCDES, 284, 292
SNCSYSACL, 418
S_TABU_DIS, 306
T000, 306
T77SO, 610, 614
T77UA, 613
TWPSSO2ACL, 486
USOBT, 572
USOBX, 572
USOBX_C, 275, 572
USREXTID, 420, 422
Task role, 571
TCP/IP, 346
Technical control, 118
Technical infrastructure, 55
Technical risk, 42
Technical user, 681
Telnet, 299
  administration service, 276, 296
  administrator, 299
Terminal server, 672
Test, 68
TGT, 141
Threat, 37
  active and passive, 36
  potential, 33
Three-system landscape, 305,
Ticket granting ticket, 141
Ticketing, 539
Time logic, 614
Token, 563
Tolerance period
  authorization, 610, 614
Tracing function, 524
Transaction, 564
  authorization management, 594
FB50, 113, 456
FBV0, 113, 456
GRMG, 525
  internal control, 321
MM01, 457
OVA7, 578
PFCG, 440, 457, 478, 516
PFUD, 577
PPOCA_BBP, 660
PPOMA_BBP, 660
RSD1, 318
RSECADMIN, 318, 319
RSSM, 316
RZ20, 524
RZ21, 525
SA38, 582
SCC4, 306
SCUA, 577
SCUG, 577
Index

SCUM, 577
SE03, 306
SE06, 306
SE16, 274, 578
SE17, 274
SE38, 258, 582
SE43, 575
SE93, 582
SICF, 301, 397, 523
SM20, 287
SM30, 274, 306, 418, 420, 422, 486
SM31, 274, 306, 578
SM36, 525
SM49, 264, 293
SM59, 283, 292, 364
SM69, 293
SMICM, 363
SNCO, 418
SP01, 586
SP02, 586
SQ01, 584
SQ02, 584
SQ03, 584
SQVI, 584
ST01, 286
STMS, 306
STRUST, 289, 299, 363, 418, 486
STRUSTSSO2, 486
SU10, 577
SU24, 572
SU53, 565
SUIM, 113, 291
SXMB_MONI, 378, 379
USERS_GEN, 663
WP3R, 477, 478
WSADMIN, 187
Transactional data, 309, 423
Transparency, 70, 72
Transport layer, 147, 180
Transport Management System, 306
Trust center, 288
Trusted connection, 552, 645
Trusted RFC connection, 665, 666
Two-factor authentication, 142, 262
TWPSSO2ACL, 486

U

UDDI, 178, 352
UME, 169, 282, 359, 388, 441, 443, 463
action, 276
administration, 430
architecture, 444
authorization concept, 281
role, 276, 282
user group, 435
UMTS, 508
Unauthorized database query, 680
Unencrypted communication, 265, 531
Unencrypted data transfer, 455
Unique user identification, 601
Universal Description, Discovery, Integration, 178, 352
Universe, 333
UNIX, 275, 305, 681
Unprotected database, 679
Unstructured data, 309
Update process, 239
Upgrade
concept, 688
missing concept, 681
Upstream control, 46
URL
filtering functionality, 392, 393, 397
generation, 432
manipulation, 526
URL blocking, 151
URL filter, 636
URM, 162
Usage
success, 239
User, 334, 427, 567, 627
administration, 590, 594
anonymous, 428, 491
certificate, 491
collection, 577
data, 577
DDIC, 263, 291
delegated administration, 472
EarlyWatch, 291
generic, 428
group, 217, 340, 584
ID, 563
indirect assignment, 675
management, 663
mapping, 471
master data, 605
master record, 217, 564
persistence storage, 281
persistence storage location, 483
persistence store, 262, 449
SAP*, 263, 291
SAP_ALL, 519, 530, 534, 650
SAP NetWeaver BW, 322
signature, 693
technical, 681
type, 217, 432, 510, 530, 534
unique identification, 601
User access, 238
User concept
SAP BusinessObjects, 333
User departments, 557
User ID, 171, 379
User Persistence Store (UPS), 76
USERS_GEN, 663
U.S. Food and Drug Administration, 93
USGAAP, 687
USOB, 572
USOB_C, 275, 319, 572
USOBX, 572
USOBX_C, 275, 319, 572
USREXTID, 420, 422
Utilities industry, 668

V

Value category, 38
Value role, 575
concept, 571, 576
Virtual Machine, 259
Virtual Private Network -> see VPN, 134, 636
Virus, 455
Virus protection, 602, 713
Virus scan, 502
Virus scanner, 526
definition file, 502
Visual administrator, 299, 301, 437
VPN, 134, 636
dial-up connection, 690
Vulnerability, 37

W

W3C, 181
Weapons law, 242
Web browser, 167, 439, 623, 701
application security, 704
cookie, 288, 485
risk and control, 702
security setting, 705
technical security, 704
Web Dynpro, 257, 267, 392
ABAP, 288, 301
application, 277, 303
Java, 288
Web front end, 384
Web service, 175, 176, 259, 347
security, 181, 186
system architecture, 180
Web Services Description Language, 177
Web Services Time Stamp, 182
WGate, 408, 412
White list, 151
Wildcard, 398
Wireless data network, 505
WLAN, 508
Work area, 226
Workbooks, 316
Workflow
management, 272
release workflow, 660
Workset, 429
World Wide Web Consortium, 181
WP3R, 477, 478
WSADMIN, 187
WSDL, 177
WS-Policy, 183
WSS10, 191
WSS11, 191
WS-SecureConversation, 191
WS-Trust, 191
This book provides a comprehensive overview of SAP NetWeaver Process Integration, revised and updated since its first edition to include information about release 7.1. Topics covered include the architecture of SAP NetWeaver PI, process design, individual runtime components, and the development of interfaces, messages, proxies, and mappings. After reading this book, you will be familiar with the essential features and technical functionality of SAP NetWeaver PI, allowing you to make the most of this useful technology.

394 pp., 2. edition 2010, 69,95 Euro / US$ 69.95

 Covers architecture, requirements, functions, and sample scenarios
 Includes discussions about the Advanced Adapter Engine, Web service integration, Services Registry, packaging, XML validation, and more
 Second edition, revised and updated for SAP NetWeaver PI 7.1

X

X.509, 451, 699
  authentication, 392
certificate, 182, 183, 287, 394, 412, 470, 489, 523, 535
client certificate, 563
  standard, 137, 287, 301, 419
xACML, 182

XI protocol, 186, 383, 385
XML, 380
digital signature, 182
encrypt messages, 376
message, 177
security standard, 182
XOR function, 128