IBM WEBSPHERE DATAPOWER SOA APPLIANCES FIRMWARE V3.8.1, SOLUTION IMPLEMENTATION COURSE CONTENT

- **SECTION 1 - FOUNDATIONAL TECHNOLOGIES (16%):**
  - A. Identify the characteristics of TCP/IP networking.
  - B. Identify the characteristics of Public Key Infrastructure (PKI).
  - C. Describe how SSL transport encryption and endpoint authentication works.
  - D. Identify the characteristics of an XML message and SOAP message.
  - E. Identify the characteristics of XSLT and XPath expressions.
  - F. Identify basic WS-Security concepts.
  - G. Identify the characteristics of attachments in web services.
  - H. Describe the characteristics of messaging systems such as WebSphere MQ and JMS.

- **SECTION 2 – ARCHITECTURE AND BASIC CONFIGURATION TASKS (16%):**
  - A. Select the appropriate WebSphere DataPower SOA Appliance based on required use case (including XA35, XS40, XI50, XI50B, XB60, XM70).
  - B. Select the appropriate usage scenarios for WebSphere DataPower Option for Application Optimization (AO).
  - C. Select the appropriate DataPower service type.
  - D. Select the appropriate message type (e.g., SOAP, XML, JSON, Pass-Thru and Non-XML).
  - E. Configure policies, request / response / error rules, and actions using the WebGUI.

- **SECTION 3 - ADMINISTRATION AND OPERATIONAL ARCHITECTURE (10%):**
  - A. Perform initial network setup and enablement of the administrative interfaces.
  - B. Create and administer users and roles on the appliance.
  - C. Implement configuration management.
  - D. Implement high availability and disaster recovery solutions as they apply to WebSphere DataPower SOA Appliances.
  - E. Configure deployment policies.
  - F. Interact with the administrative interfaces (CLI, WebGUI, XML Management).

- **SECTION 4 - SECURITY SCENARIOS (18%):**
  - A. Configure a service to secure a WSDL-described web service.
  - B. Configure a service to enforce non-repudiation using digital signatures.
  - C. Configure a service to enforce confidentiality using encryption.
  - D. Configure a service to enforce authentication and authorization.
  - E. Configure XML threat protection.
  - F. Configure a service to use SSL.

- **SECTION 5 - INTEGRATION SCENARIOS (18%):**
  - A. Configure a service Front Side Protocol Handler.
  - B. Configure a service Backend URL.
  - C. Configure a service for mediation between protocols.
  - D. Configure a service for integration with messaging systems such as WebSphere MQ, WebSphere JMS and TIBCO EMS.
  - E. Configure a service to perform XML and Non-XML message transformation using the Transform actions.
  - F. Configure a service for Web 2.0 scenarios.
  - G. Configure a service for database integration.

- **SECTION 6 – SOA GOVERNANCE SCENARIOS (7%):**
  - A. Configure SLM statements on a service to enforce granular service levels.
  - B. Attach and enforce WS-Policy statements using a WS-Proxy service.

C. Configure subscriptions to external service registries.

❖ **SECTION 7 - TROUBLESHOOTING (15%):**

A. Resolve network connectivity problems.
B. Perform and analyze packet captures.
C. Configure Log Targets for analysis and alerting.
D. Configure event triggers.
E. Analyze system logs.
F. Debug message flows using the Probe.
G. Configure a service for transaction logging.