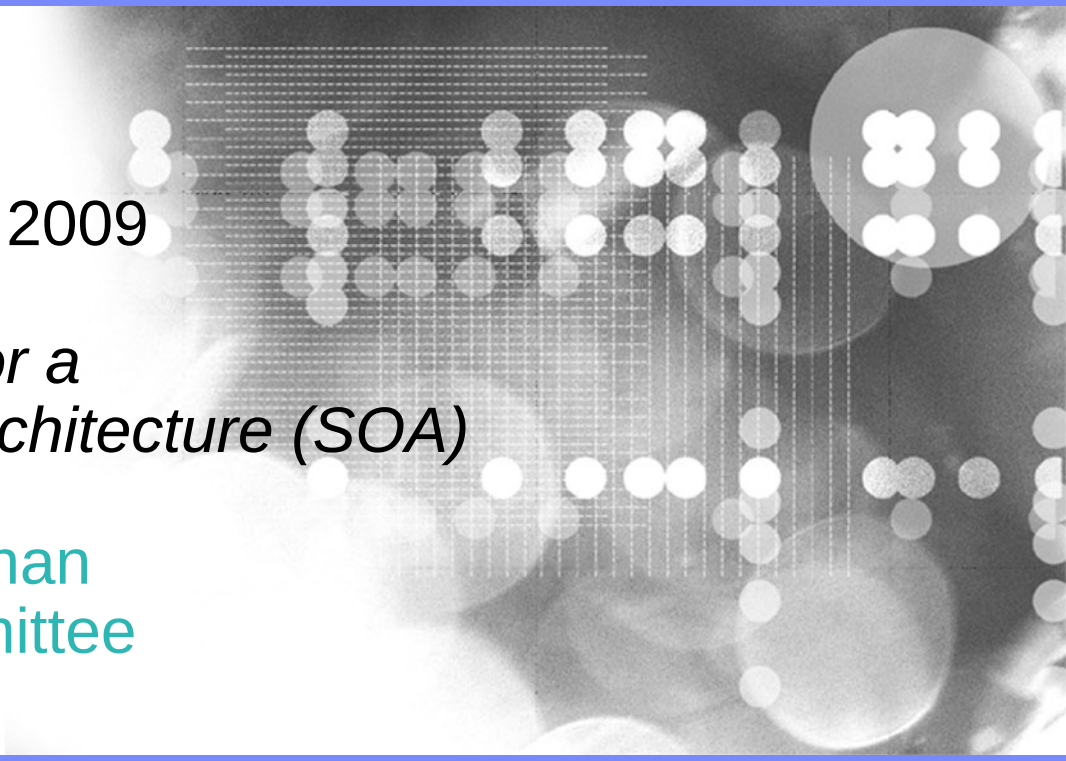
z/TPF V1.1



TPF Users Group - Spring 2009

z/TPF Security Features for a Service Oriented Architecture (SOA)

Jason Keenaghan
SOA Subcommittee

AIM Enterprise Platform Software
IBM z/Transaction Processing Facility Enterprise Edition 1.1.0

Agenda

- **z/TPF Web services infrastructure**
- **z/TPF security infrastructure**
- **WS-Security for z/TPF: Bringing it all together**
- **SOA deliverables update**

The basics about Web services support on z/TPF

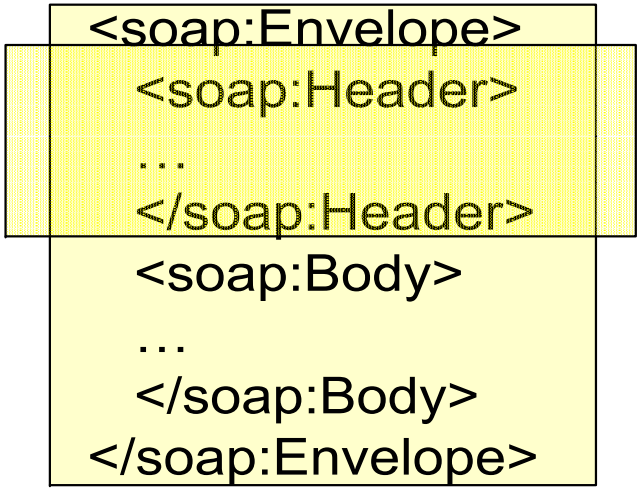
- **Communications bindings…**
  - Receive SOAP requests from the network and pass them to the z/TPF SOAP handler for processing
  - Return SOAP responses to the original requester across the network
  - Sample bindings include: Apache 1.3 and Apache 2.2 HTTP servers, WebSphere MQ
- **z/TPF SOAP handler…**
  - Is responsible for message translation, XML parsing, SOAP syntax checking, and message routing

Creating a provider Web service for z/TPF

- **4 primary *artifacts* that each provider Web service should have:**
  - **WSDL document:** defines the interface to the Web service for Web service consumers
  - **Provider Web service deployment descriptor:** defines the runtime characteristics of the Web service to the z/TPF SOAP handler
  - **Web service wrapper program:** processes the SOAP request message, invokes the Web service application, constructs the SOAP response message
  - **Web service application:** provides the actual service being requested

Extending the basic Web services support

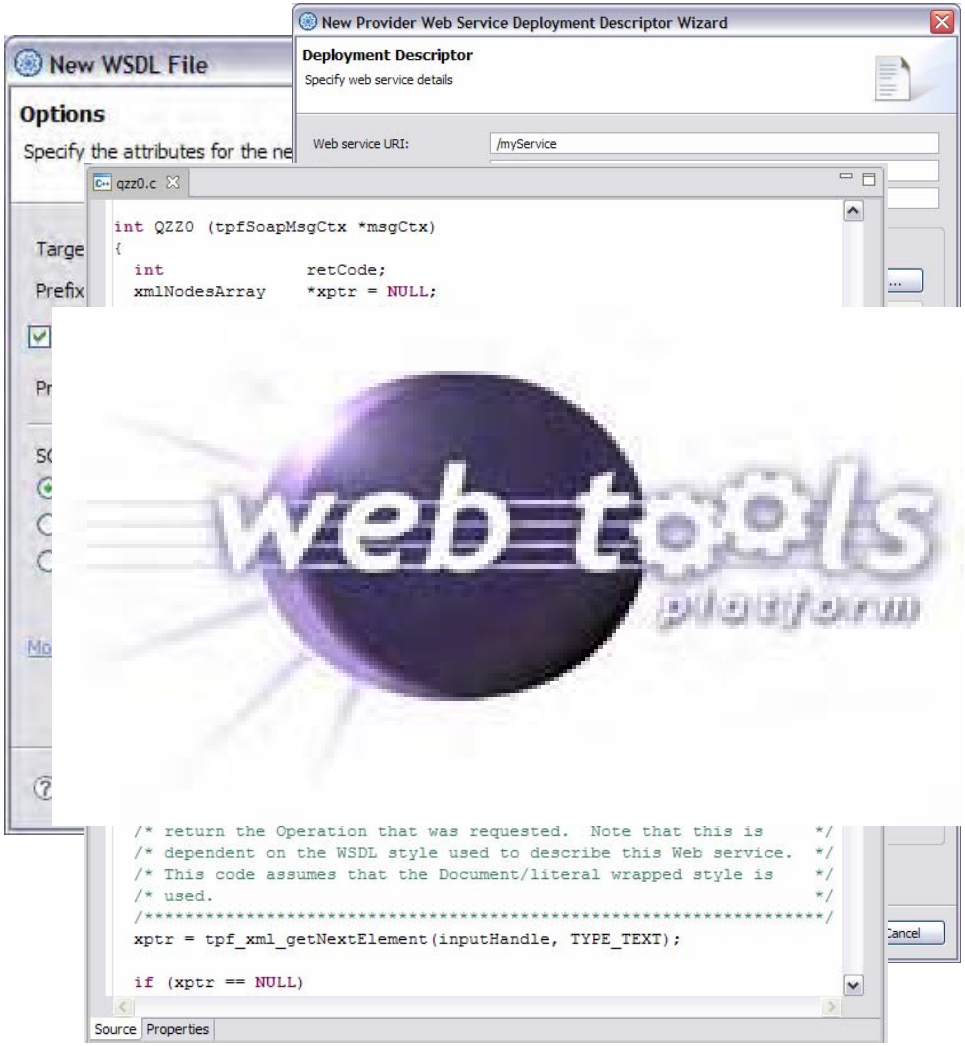
- **The SOAP specifications allow for a great deal of extensibility by using the "Header" section of SOAP messages**
- **A large number of secondary specifications have evolved for solving common business problems; collectively, these are known as** *SOAP features* **or** *WS-**
  - WS-Security
  - WS-Addressing
  - WS-Reliable Messaging



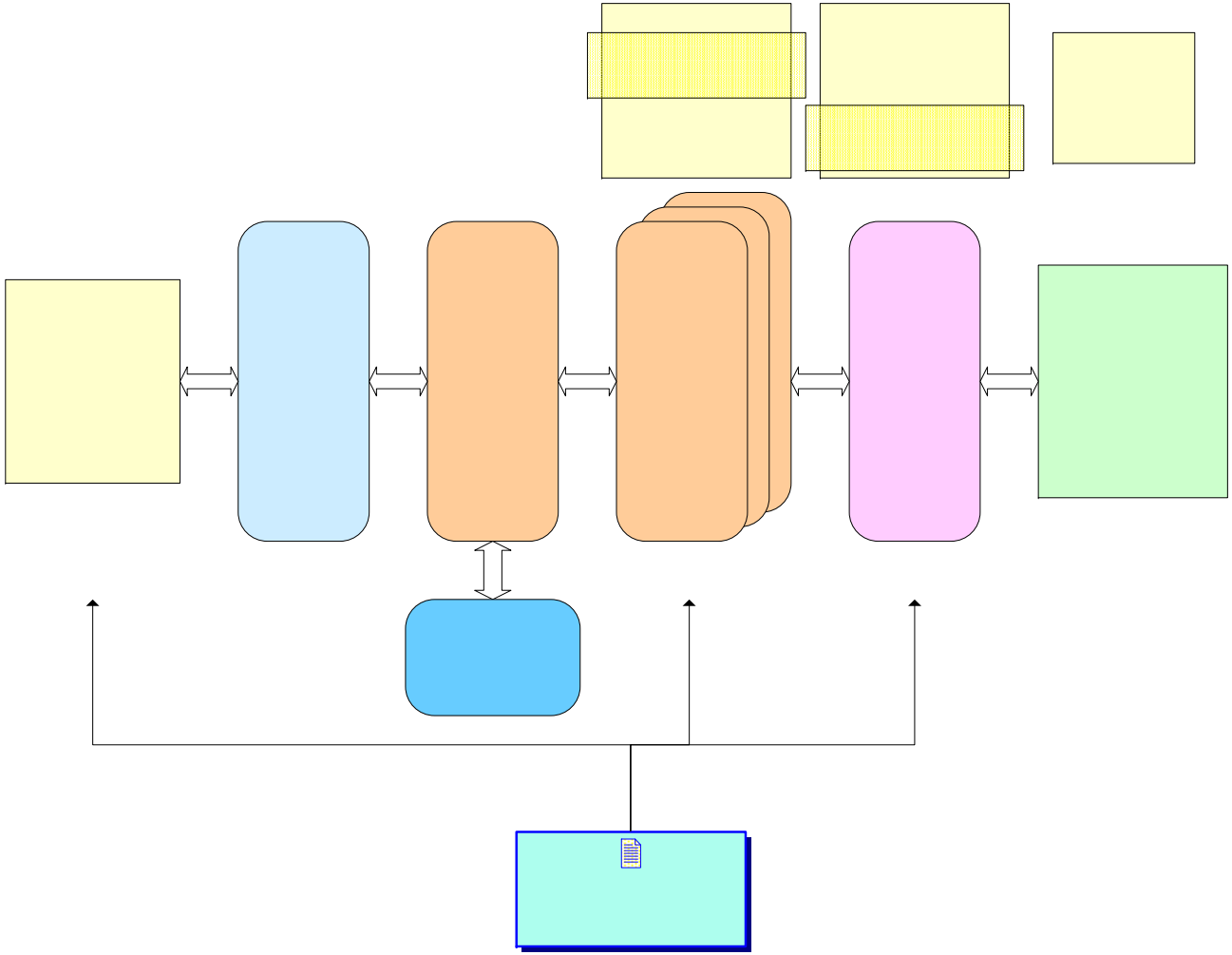
z/TPF contains infrastructure for you to create reusable Web service extensions, known on z/TPF as *SOAP message handlers*

Web service development is easier with tooling

- **IBM TPF Toolkit greatly simplifies the steps required to create a Web service for z/TPF**
- **Automation and tooling exists for creating artifacts needed for Web service creation and deployment**
- **Web Tools Platform (WTP) Eclipse plug-in integrated in IBM TPF Toolkit:**
  - XML editor
  - WSDL editor
  - WSIL creation wizard
  - Publish WSDL documents to UDDI registry
  - Web services explorer (SOAP client for testing)



Logical processing flow of a SOAP request

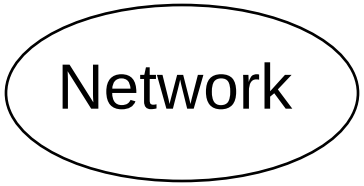


Agenda

- **z/TPF Web services infrastructure**
- **z/TPF security infrastructure**
- **WS-Security for z/TPF: Bringing it all together**
- **SOA deliverables update**

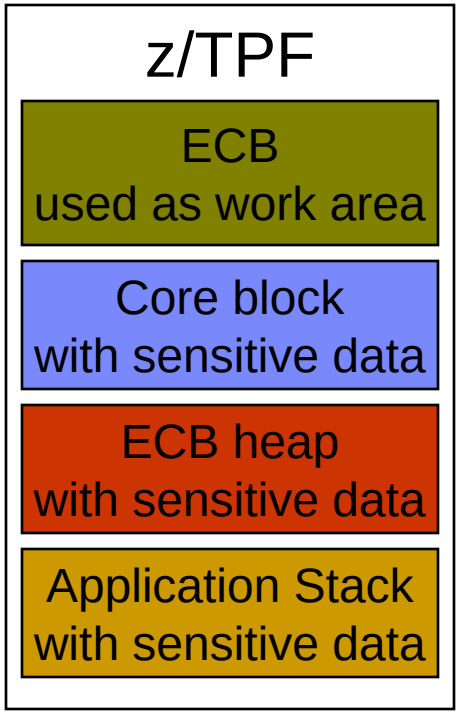
z/TPF data security support

Data in flight



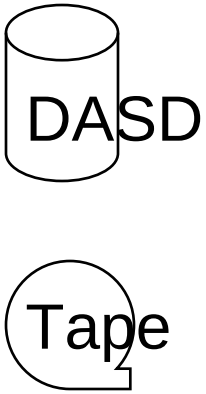
Sensitive data encrypted when transmitted over the network.

Data in use



Sensitive data needs to be secure when it is being used.

Data at rest



Sensitive data encrypted when saved on DASD or on tape.

Securing data in flight

- **OpenSSL**
  - Hardware acceleration for starting SSL sessions
    - Using PCICA (PUT 2)
    - Using CEX2A (PUT 2)
  - AES cipher suites for SSL (PUT 3)
  - Hardware acceleration for SSL data messages using CPACF
    - DES, TDES, SHA-1 (PUT 2)
    - AES-128 (PUT 3)
    - AES-256 (PUT 5)
  - PKI support (PUT 6)
- **Secure FTP client (PUT 3)**
  - Makes use of the CURL open source library
- **Secure HTTP client (PUT 4)**
  - Makes use of the CURL open source library
- **Secure HTTP server (PUT 5)**
  - Makes use of the Apache 2.2 open source HTTP server
- **z/TPF WebSphere MQ Support for SSL (coming soon)**

Securing data in use

- **Nondisplayable ECB storage support**
- **Prevent areas of working storage from being displayed:**
  - Dumps will not display data
    - Dumps will include a list of nondisplayable areas
  - Commands like ZDCOR / ZDDCA will not display data
  - Debugger will not display data
  - Data will be displayed as ********
- **Pass nondisplayable storage from one ECB to another**

Securing data at rest

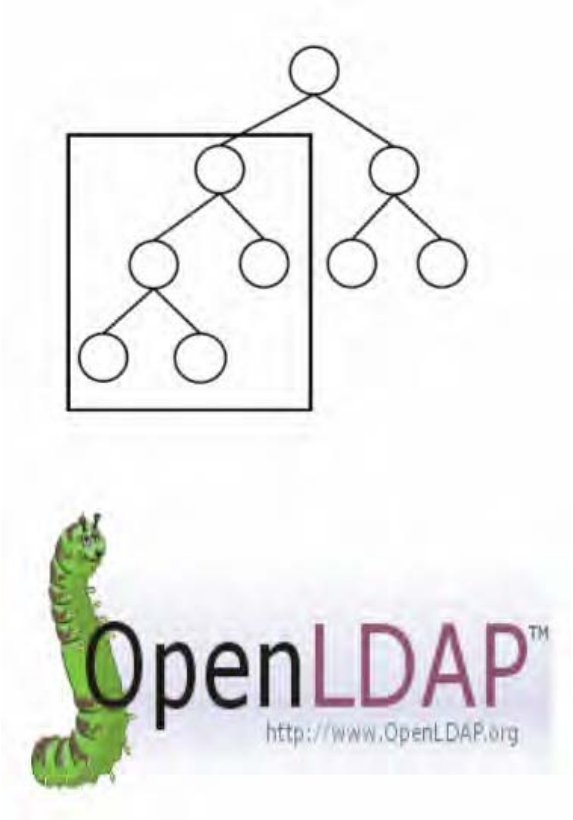
- **Tape hardware encryption (IBM TS1120 encrypted tape drives)**
  - Ability to mount output tapes as encrypted
    - Tape control unit encrypts the data before writing it to the tape
  - Ability to read encrypted tapes
    - Tape control unit communicates with its key manager to obtain the necessary decryption key
  - Encrypted tapes allow tapes containing sensitive data to:
    - Leave the data center (archive, exchange data with business partners)
    - Be stored locally and control access to that data
- **z/TPF-unique encryption/digest APIs**
  - Exploit System z hardware acceleration for: DES, TDES, AES-128, AES-256, SHA-1, SHA-256

z/TPF secure key stores

- **Secure key management**
  - Enables you to create and manage symmetric encryption keys in a secure manner
  - Applications can use the support to protect sensitive data stored on tape or disk (data at rest) or flowing over the network (data in flight)
  - High performance designed for mainline application use
  - Access controls to limit and log key usage
  - Can help you meet the ever growing list of security and compliance standards
- **Public Key Infrastructure (PKI) support**
  - Ability to create/manage RSA key pairs on z/TPF in a secure manner, similar to how existing secure key management support handles symmetric keys
    - RSA private keys are protected via the key store
  - Ability to create digital certificate requests
    - Using z/TPF generated RSA public key as input
  - Enable SSL applications to use z/TPF generated RSA key pairs
  - Secure key import
    - Ability to import a symmetric key in a secure manner from a remote key manager using RSA key wrapping

OpenLDAP on z/TPF

- **Lightweight Directory Access Protocol (LDAP)**
  - LDAP is an approved Internet standard
  - LDAP defines specific directory behavior as well as the underlying TCP/IP communication protocol used in client/server interaction
- **Directories are widely used as a repository to store user authentication and authorization information**
- **OpenLDAP is an open source implementation of the LDAP standard available to run on z/TPF (PUT 5)**



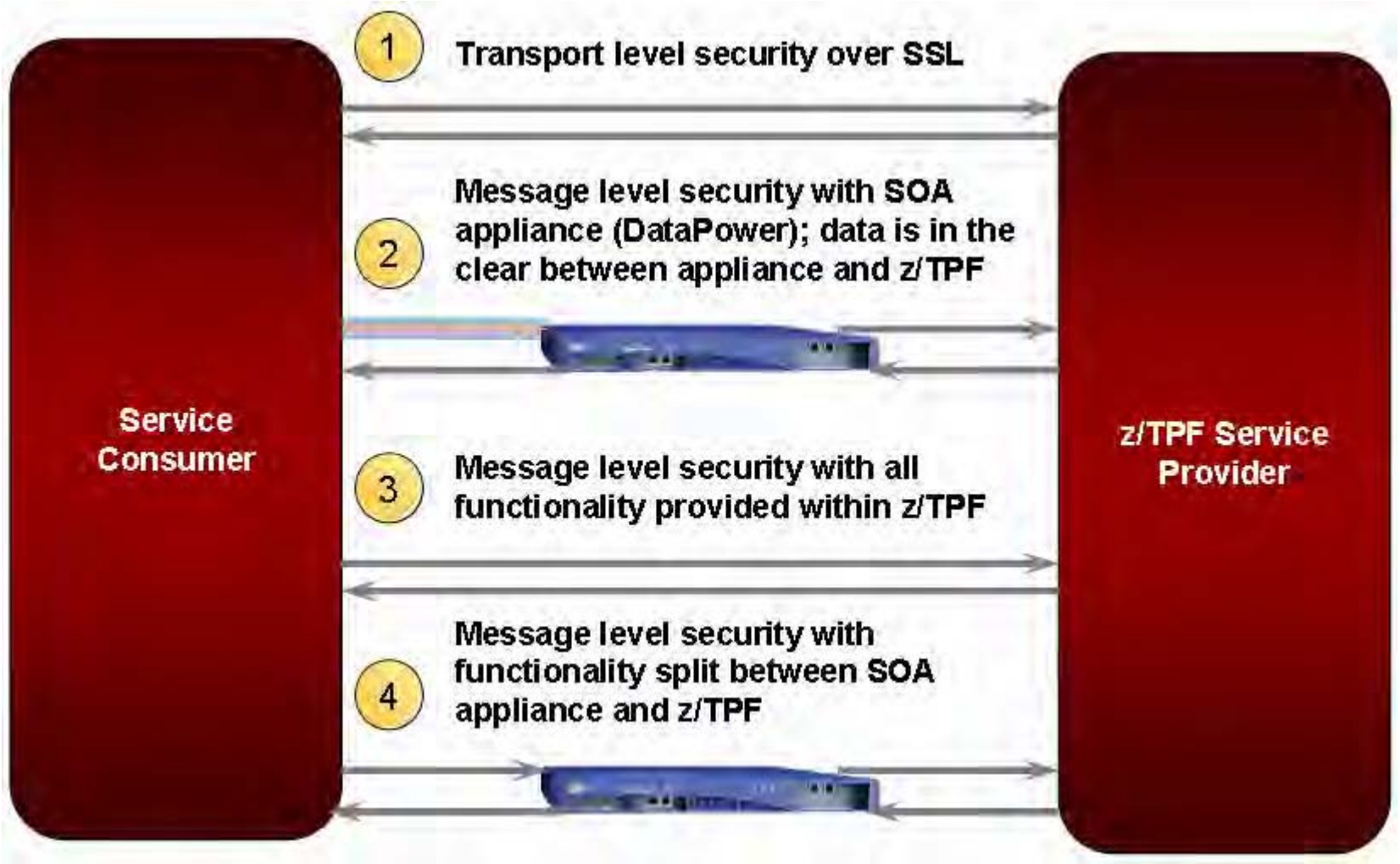
Agenda

- **z/TPF Web services infrastructure**
- **z/TPF security infrastructure**
- **WS-Security for z/TPF: Bringing it all together**
- **SOA deliverables update**

Disclaimer

- **The information that follows represents design concepts only for possible additions to the z/TPF product.**
- **The information is provided for planning purposes only.**
- **IBM reserves the right to change these plans at its discretion.**
- **Any reliance on such a disclosure is solely at your own risk.**
- **IBM makes no commitment to provide additional information in the future.**

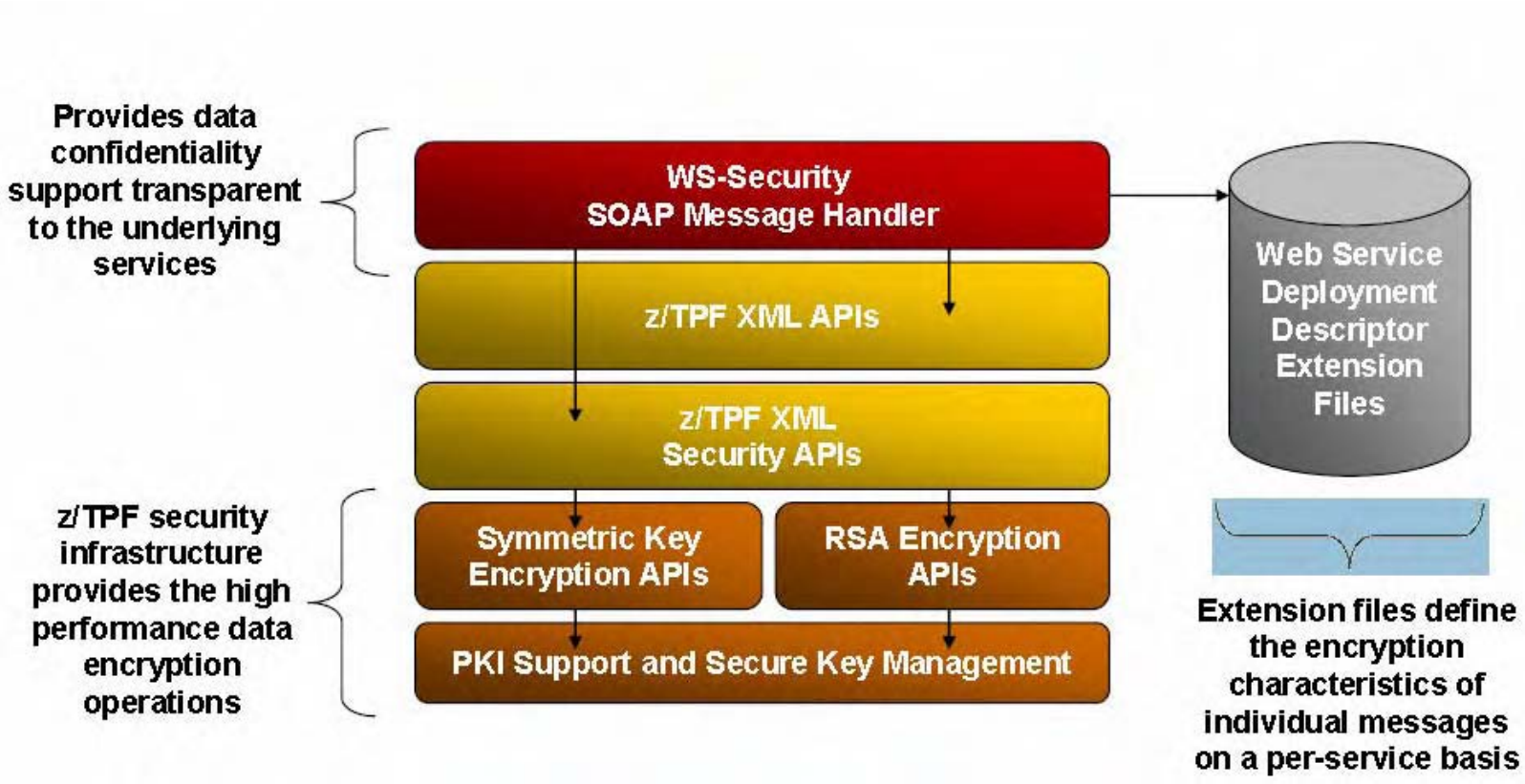
Four options for Web services security on z/TPF



Data confidentiality: XML Encryption

- **Open standard developed by the World Wide Web Consortium (W3C) specifies a process for encrypting data and representing the result in XML**
- **z/TPF direction - Provide a set of XML Security APIs that can be used by any application to do the following:**
  - Encrypt an XML element or element content using the specified encryption algorithm and key information; create the corresponding `<EncryptedData>` element in the XML structure
  - Encrypt a symmetric key that was used to encrypt an XML element or element content using the specified encryption algorithm and key information; create the corresponding `<EncryptedKey>` element in the XML structure
  - Decrypt an `<EncryptedData>` or `<EncryptedKey>` element and update the corresponding XML structure with the results; decrypted data is stored in the XML structure in ECB heap storage marked as non-displayable

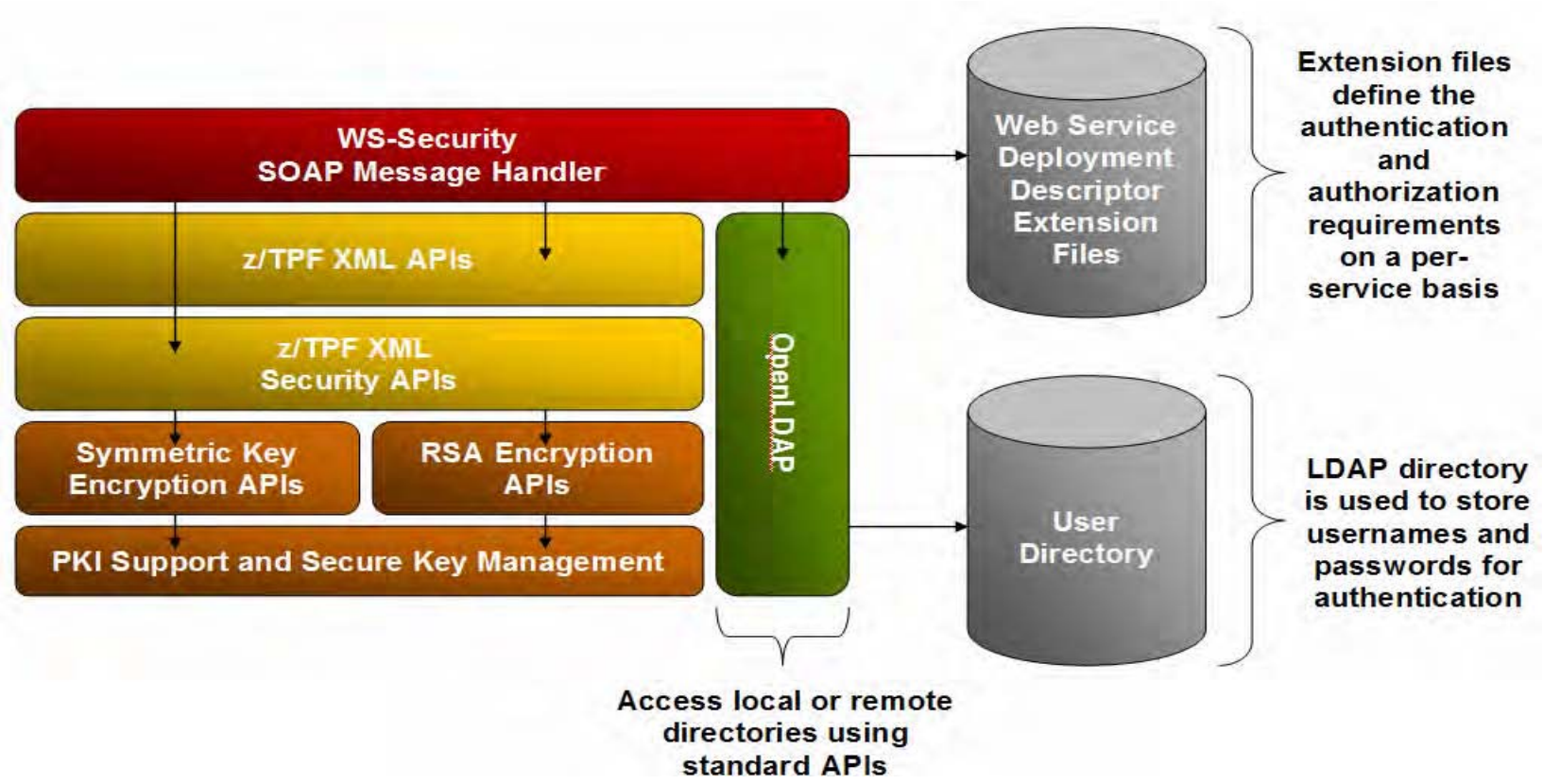
WS-Security SOAP message handler (Phase 1)



Authentication & Authorization: Username Token

- **WS-Security defines several different supplemental specifications that can be used for user identification: Username Token, SAML Token, X.509 Binary Tokens, and others**
- **Username Token support uses a combination of usernames and passwords for authentiction**
- **Passwords may be specified: in the clear, as a digest, or as a digest using a nonce and creation timestamps**
- **z/TPF direction - Provide an extensible mechanism to identify and verify usernames in SOAP Security header blocks and insert usernames/passwords in outbound SOAP messages**
  - LDAP-based user directory
  - File system password and group files
  - User-implemented authentication and authorization

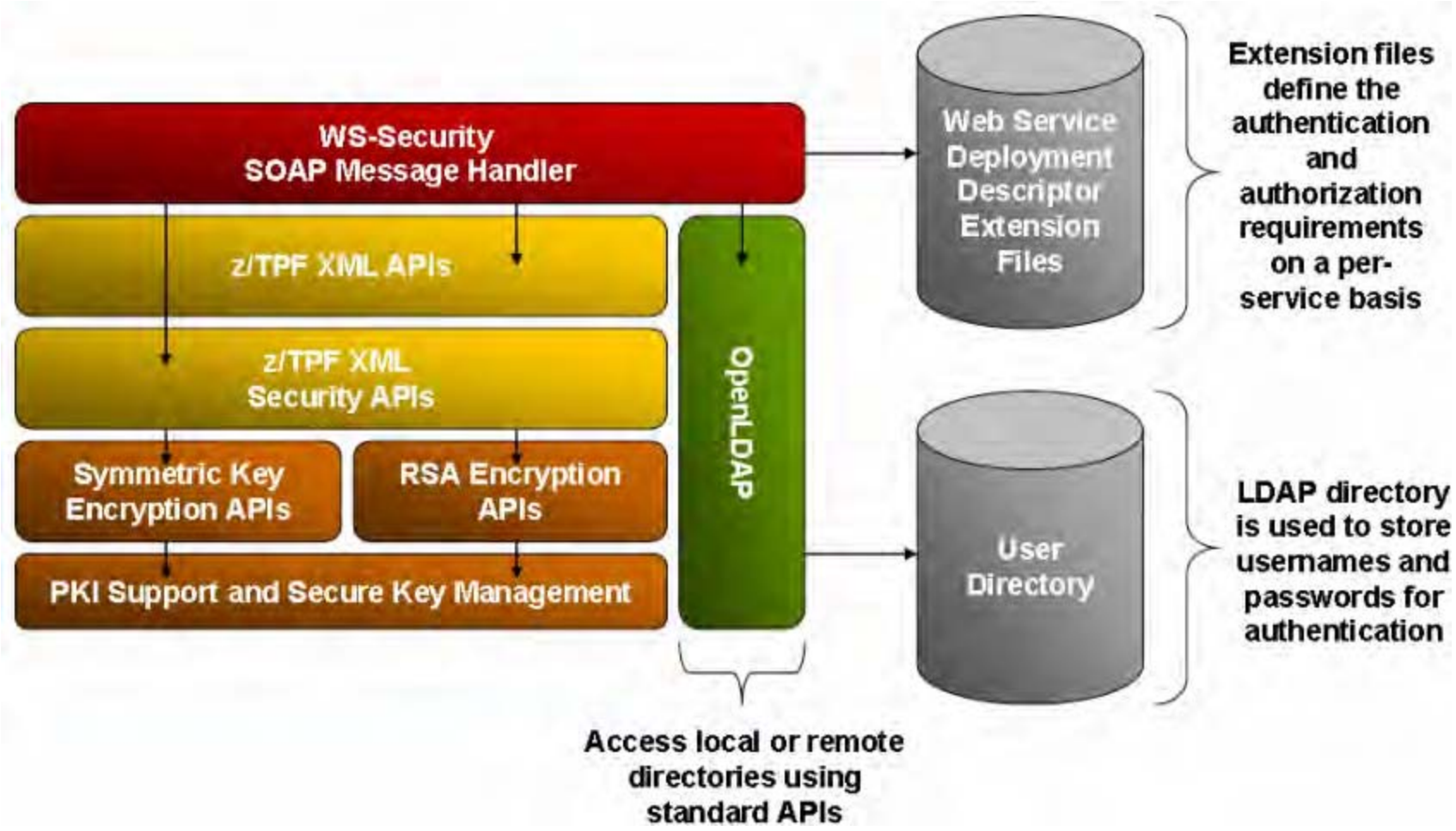
WS-Security SOAP message handler (Phase 2)



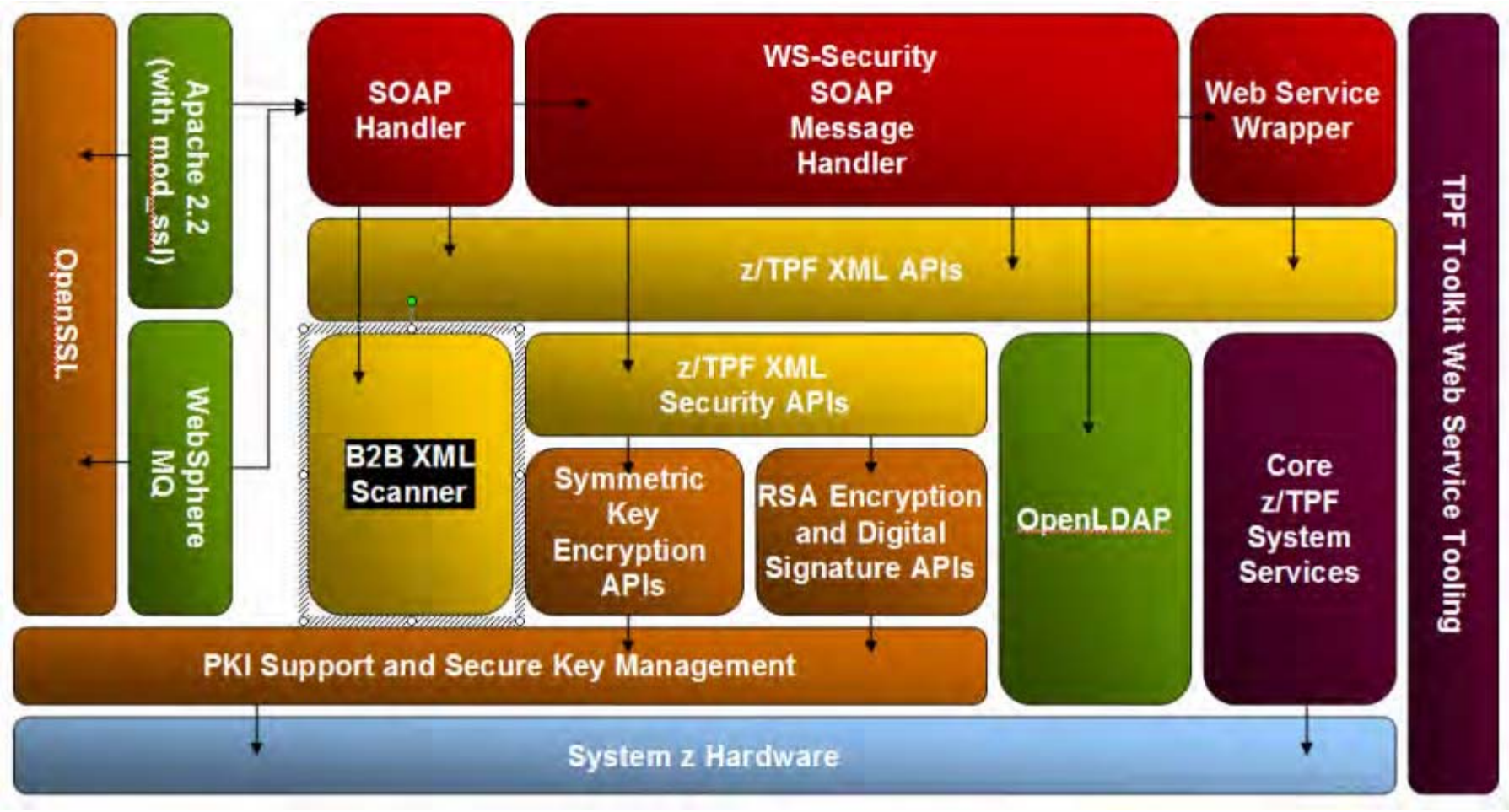
Data integrity: XML Digital Signature

- **Open standard developed by the World Wide Web Consortium (W3C) specifies a process for digitally signing portions of an XML document and representing the result in XML**
- **Because digital signature processing is based on RSA encryption, it is a very costly operation**
- **The TPF development lab is looking for user input about whether or not having the support native on z/TPF is required, or if an off-board SOA appliance is more desirable**
- **z/TPF direction - If the support is provided natively on z/TPF, expect a set of XML Security APIs that could be used by any application to do the following:**
  - Generate and insert a `<Signature>` element based on the portion of the XML document to be signed as specified by the user
  - Verify a `<Signature>` element within an XML document

WS-Security SOAP message handler (Phase 3)



Roadmap for Web services security on z/TPF

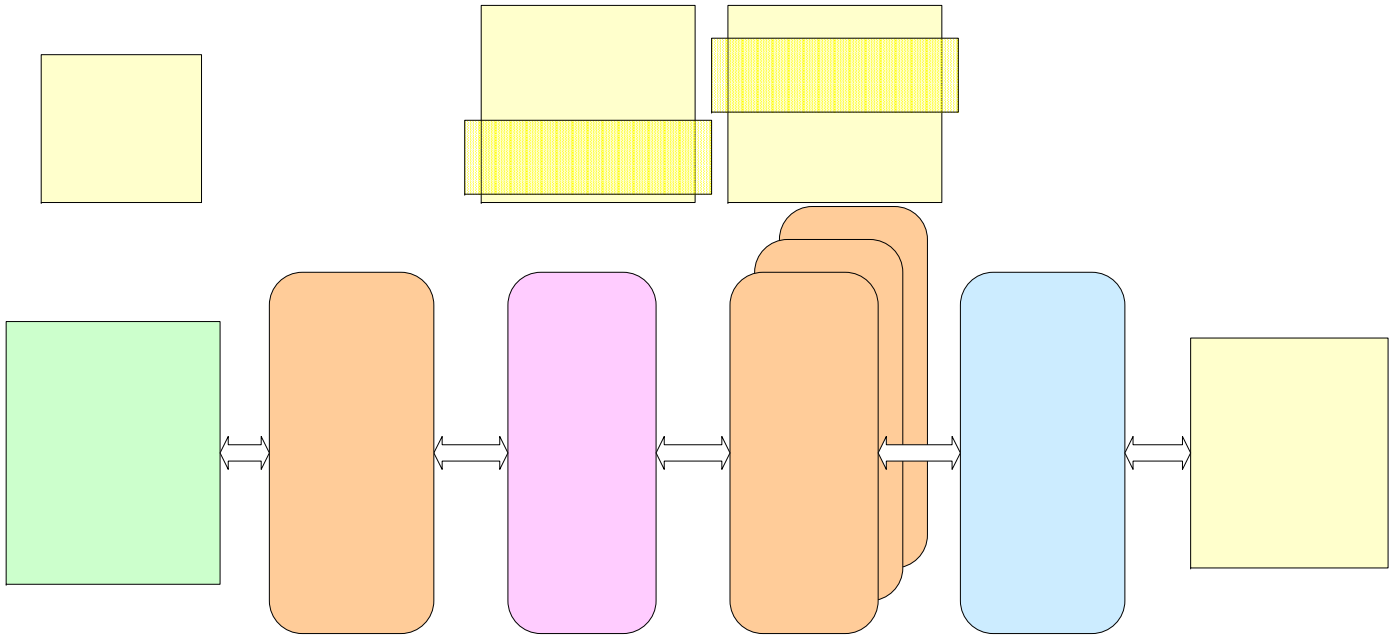


Agenda

- **z/TPF Web services infrastructure**
- **z/TPF security infrastructure**
- **WS-Security for z/TPF: Bringing it all together**
- **SOA deliverables update**

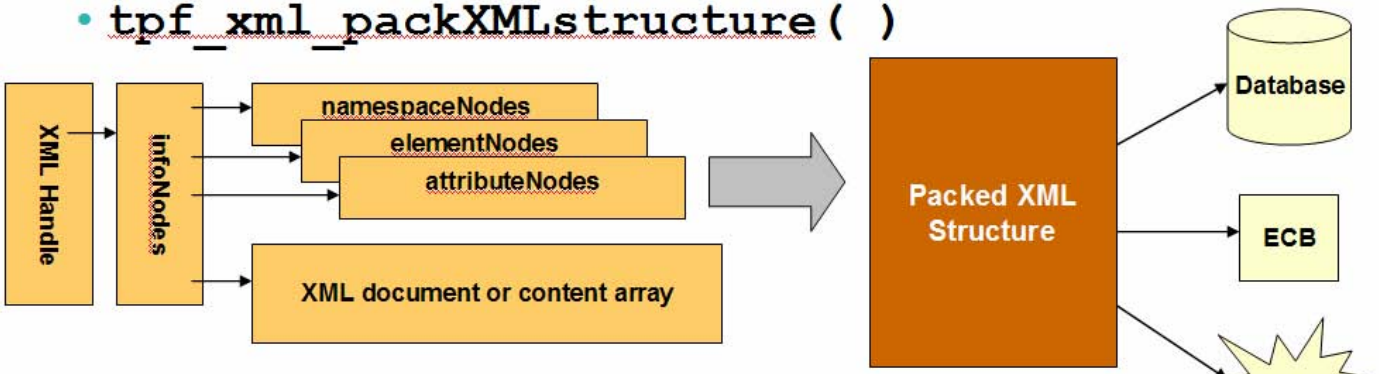
SOAP consumer support (PJ35511) – Just released

- **Consists of a set of z/TPF unique APIs that can be used by applications to easily send SOAP-based Web service requests to service providers**
- **Builds upon existing Web service deployment mechanisms and Web service tooling support released on z/TPF PUT 4**
- **Makes available the following TPFUG requirements: A004001 and DS07001F**

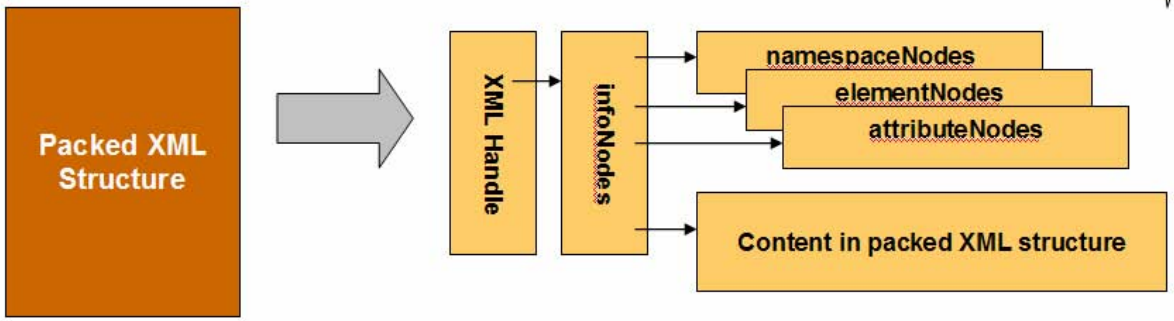


Additional XML API updates available in PJ35511

- tpf_xml_packXMLstructure( )



- tpf_xml_initialize_handle( )



Even more XML API updates available in PJ35511

- **`tpf_xml_insertBinaryElement( )` and `tpf_xml_appendBinaryElement( )`**
  - Binary data is added to XML structure as-is
  - Data is only base64 encoded or hex encoded when `tpf_xml_buildXMLdocument()` is called
- **`tpf_xml_get*` functions accept new `TYPE_BASE64_BINARY` and `TYPE_HEX_BINARY` to perform text-to-binary data conversion**

SOAP consumer support and WS-Security

- **All of the security features previously described in the context of provider Web services will also be usable by consumer Web services**
- **Similar deployment descriptor extension files will control the security requirements of outbound SOAP request messages as well as the processing of inbound SOAP responses**

Trademarks

- **IBM, and DataPower are trademarks of International Business Machines Corporation in the United States, other countries, or both.**
- **OpenLDAP is a registered trademark of the OpenLDAP Foundation.**
- **OpenSSL is a trademark of The OpenSSL Project.**
- **Other company, product, or service names may be trademarks or service marks of others.**

- **Notes**
- **Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.**
- **All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.**
- **This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.**

- **All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.**

- **Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.**

- **Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.**

- **This presentation and the claims outlined in it were reviewed for compliance with US law. Adaptations of these claims for use in other geographies must be reviewed by the local country counsel for compliance with local laws.**