z/TPF V1.1

TPF Users Group - Fall 2009
Data Confidentiality for Web Services (WS-Security on z/TPF)

Direction

Aleksandr Krymer
SOA Subcommittee

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

Agenda

- **Brief introduction to WS-Security and XML Encryption**
- **Overview of existing SOAP support**
- **Planned data confidentiality support for Web Services on z/TPF**
- **Questions**

Web services security (WS-Security)

- **WS-Security is made up of a collection of specifications:**
  - WS-Security Core Specification 1.1 (link)
  - Username Token Profile 1.1 (link)
  - X.509 Token Profile 1.1 (link)
  - SAML Token Profile 1.1 (link)
  - Kerberos Token Profile 1.1 (link)
  - Rights Expression Language (REL) Token Profile 1.1 (link)
  - SOAP with Attachments (SwA) Profile 1.1 (link)
- **WS-Security also builds upon other specifications:**
  - XML encryption (XMLENC) (link)
  - XML digital signatures (XMLDSIG) (link)
  - Canonical XML Version 1.0 (XMLC14N) (link)
  - Exclusive XML Canonicalization Version 1.0 (EXCC14N) (link)
- **Web Services Interoperability Organization (WS-I) clarifies WS-Security:**
  - Basic Security Profile 1.0 (link)

XML encryption

- **Open standard developed by the World Wide Web Consortium (W3C)**
- **Standard specifies the following:**
  - Steps to encrypt data
  - Steps to decrypt encrypted data
  - Syntax to represent XML encrypted data, the information used to decrypt the data, and a list of encryption algorithms supported
- **Data being encrypted/decrypted in an XML document may be either:**
  - Arbitrary data (including an entire XML document)
  - An XML element (including child elements if any)
  - XML element content (which may be character data, or all child elements)
- **Result of encrypting data is an <EncryptedData> element which contains (via one of its children's content) or identifies (via a URI reference) the cipher data**
  - When encrypting an XML element or element content the <EncryptedData> element replaces the element or content in the encrypted version of the XML document
  - When encrypting arbitrary data (including entire XML documents), the <EncryptedData> element may become the root of a new XML document or become a child element in an application-chosen XML document

WS-Security usage of XML encryption standard

- **WS-Security Core Specification (WSSE) allows for encryption of any combination of body blocks, header blocks, and any of these sub-structures**
- **WS-Security defines a `<wsse:Security>` header block where all security related information should be inserted, including information about message encryption**
  - When a producer or active-intermediary encrypts portion(s) of a SOAP message it must prepend a sub-element to the `<wsse:Security>` header block
  - The sub-element MUST contain the information necessary for the recipient to identify the portions of the message that it is able to decrypt
- **WS-Security also defines a new element called `<wsse11:EncryptedHeader>` for containing encrypted header blocks (similar to `<EncryptedData>` element of XMLENC)**

Identifying encrypted data in SOAP messages

- **<ReferenceList> element usage in <wsse:Security> header block**
  - May be used to create a manifest of encrypted portions within the SOAP envelope
  - All <EncryptedData> elements created should be listed in <DataReference> elements inside one or more <ReferenceList> elements

```
<S11:Envelope xmlns:S11="..."
  xmlns:wsse="...
      xmlns:wsu="..." xmlns:ds="..."
  xmlns:xenc="...">
  <S11:Header>
     <wsse:Security>
        <xenc:ReferenceList>
           <xenc:DataReference
                 URI="#bodyID"/>
        </xenc:ReferenceList>
     </wsse:Security>
  </S11:Header>
  <S11:Body>
     <xenc:EncryptedData Id="bodyID">
        <ds:KeyInfo>
           <ds:KeyName>
           CN=Hiroshi Maruyama,C=JP
           </ds:KeyName>
        </ds:KeyInfo>
        <xenc:CipherData>
           <xenc:CipherValue>
           ...
           </xenc:CipherValue>
        </xenc:CipherData>
     </xenc:EncryptedData>
  </S11:Body>

</S11:Envelope>
```

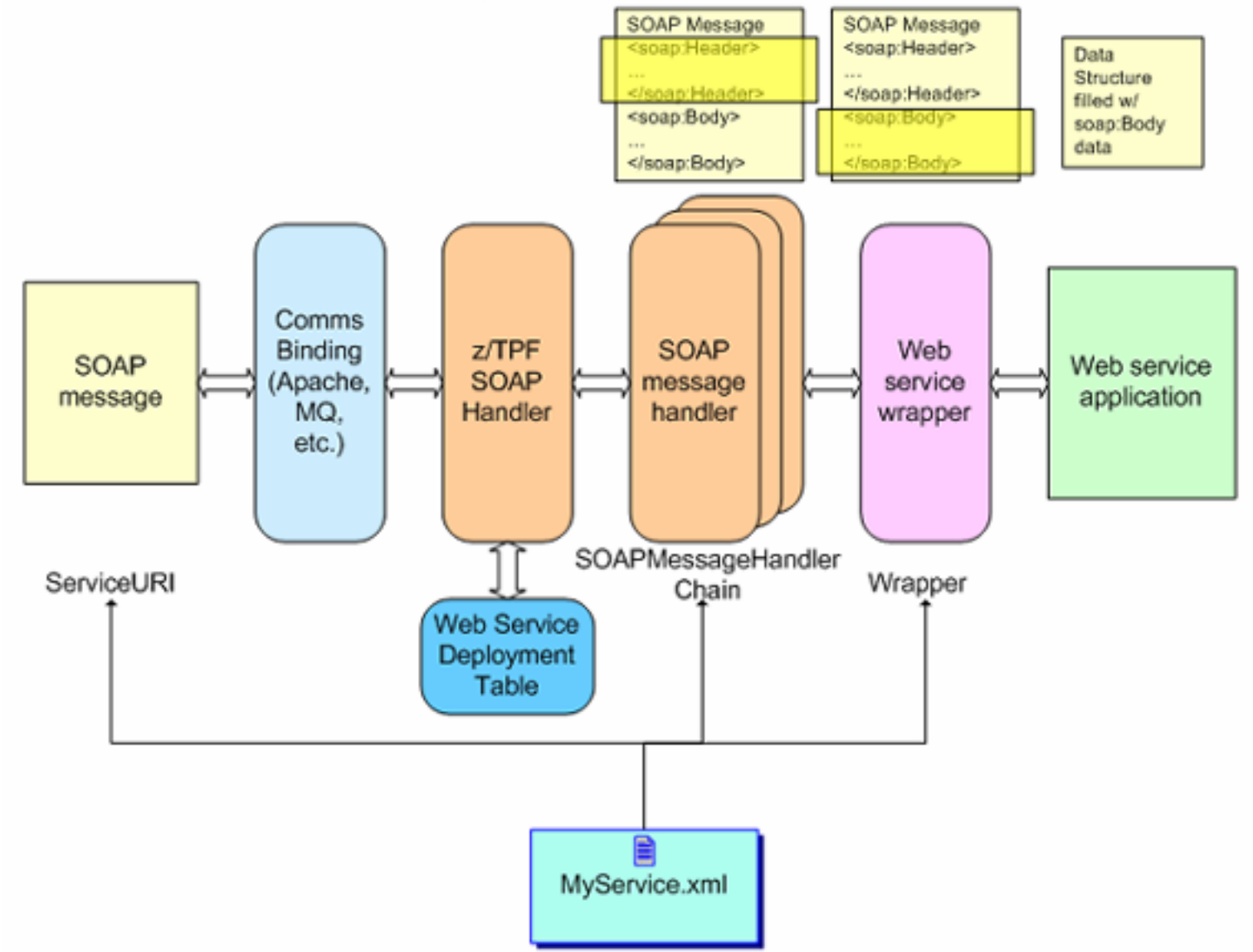
Identifying symmetric keys in SOAP messages

- **Use either a 'common' key (i.e., reference a key by name) or encrypt the key itself in the SOAP message**
- **Encrypted keys are carried in the `<EncryptedKey>` element**
  - This element may also contain a `<ReferenceList>` that identifies the portions of the message that are encrypted with this key
  - `<ReferenceList>` can occur outside of this element, as long as the `<EncryptedData>` in question has a `<KeyInfo>` element that references this key

Additional information about encryption with SOAP

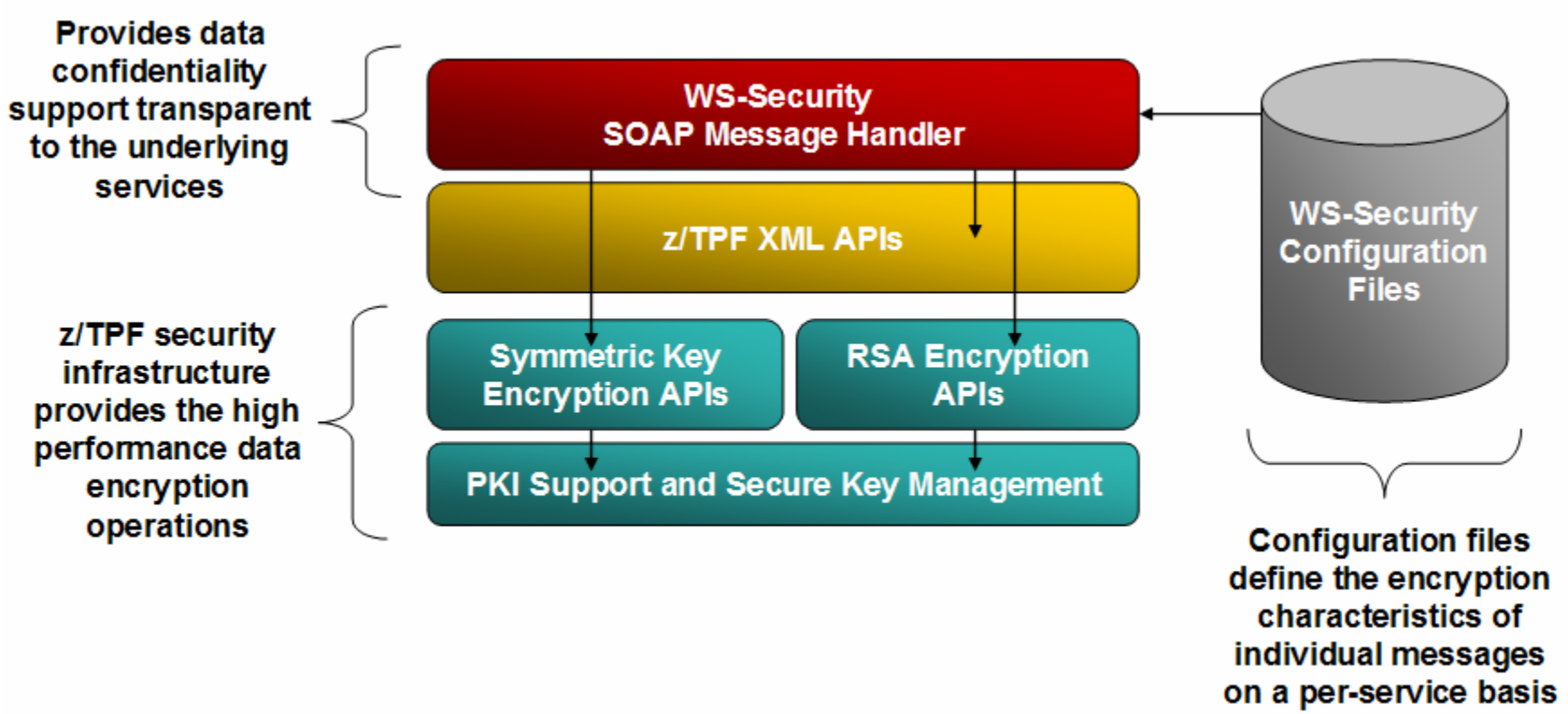
- **<Envelope>, <Header>, and <Body> elements must not be encrypted, although child elements may be encrypted**
- **Multiple steps of encryption may be added in a single <wsse:Security> header block if they are targeted for the same recipient**

Overview of existing SOAP support



WS-Security SOAP message handler for z/TPF

Direction



Planned Data Confidentiality Support for Web Services
Direction

- **Protected sensitive data**
  - Non-displayable storage for all decrypted information
  - Mechanism to specify sensitive data fields in unencrypted SOAP message
- **Field-level encryption configuration**
- **Super-encryption support**
  - Encrypting encrypted data
- **TPF Toolkit support**
  - Deployment descriptor updates
  - Configuration file wizard

Planned Data Confidentiality Support for Web Services - keys
Direction

- **Shared symmetric keys** — **work in progress**
- **Session-level key wrapping** — **future work**
- **Session-level key transport** — **future work**
- **User-specified keys** — **future work**
- **Key types:**
  - AES-128-CBC
  - AES-256-CBC
  - TDES
  - RSA v1.5

Data Confidentiality Support for Web Services – configuration

Direction

- **Inflow**
  - Which encrypted fields must be present in the request
- **Outflow and Faultflow**
  - Which fields need to be encrypted
    - Identified by a subset of XPath
  - Which keys need to be used
    - z/TPF keystore
    - Generated for the session
    - Specified in user exit
  - How keys are transported
    - Common alias specified in the message
    - Encrypted using shared symmetric key or public key and sent as part of the message

Data Confidentiality Support for Web Services – configuration (cont)

Direction

- **How to match keys used on both sides?**
  - Key alias on z/TPF
    - New Z-command
    - Actual key name in z/TPF keystore depends on the key alias AND the destination
    - Alternatively, use user exit to map alias to the key
  - Away from z/TPF
    - Maintain a mapping between actual key names and key aliases specified in SOAP messages
      - Similar to existing SOAP engines, like Apache Axis2

Data Confidentiality Support for Web Services on z/TPF – how to enable this support?

Direction

- **Changes to existing applications**
  - NONE
- **Deploy WS-Security SOAP message handler**
- **For each Web service that requires WS-Security**
  - Create an configuration file with encryption parameters
  - Add WS-Security to SOAP message handler chain and specify the configuration file name
  - Redeploy the service

Questions? Comments?

Trademarks

- IBM is a trademark of International Business Machines Corporation in the United States, other countries, or both.
- 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.