TLS Support for z/TPF High Speed Connector and Enhanced HTTP Client

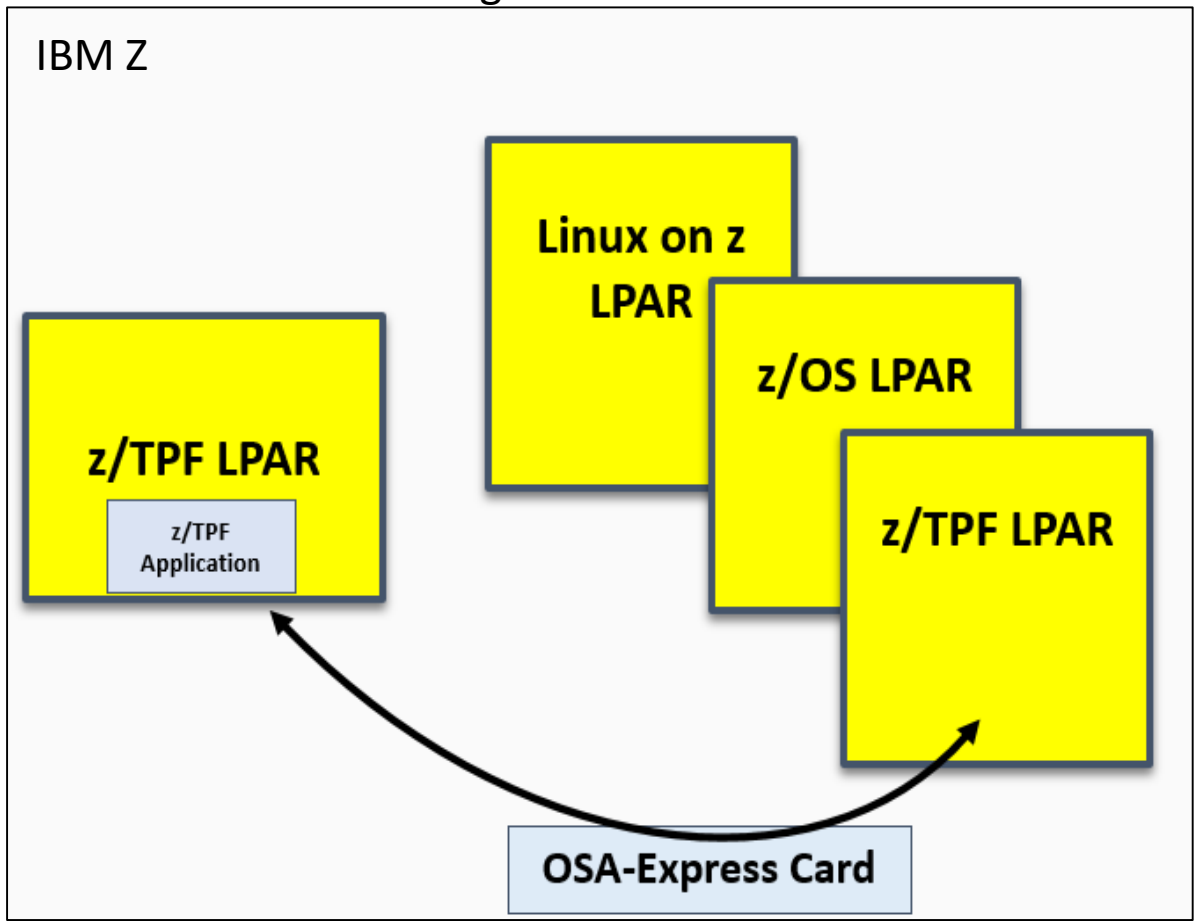
Jamie Farmer
z/TPF Development

Agenda

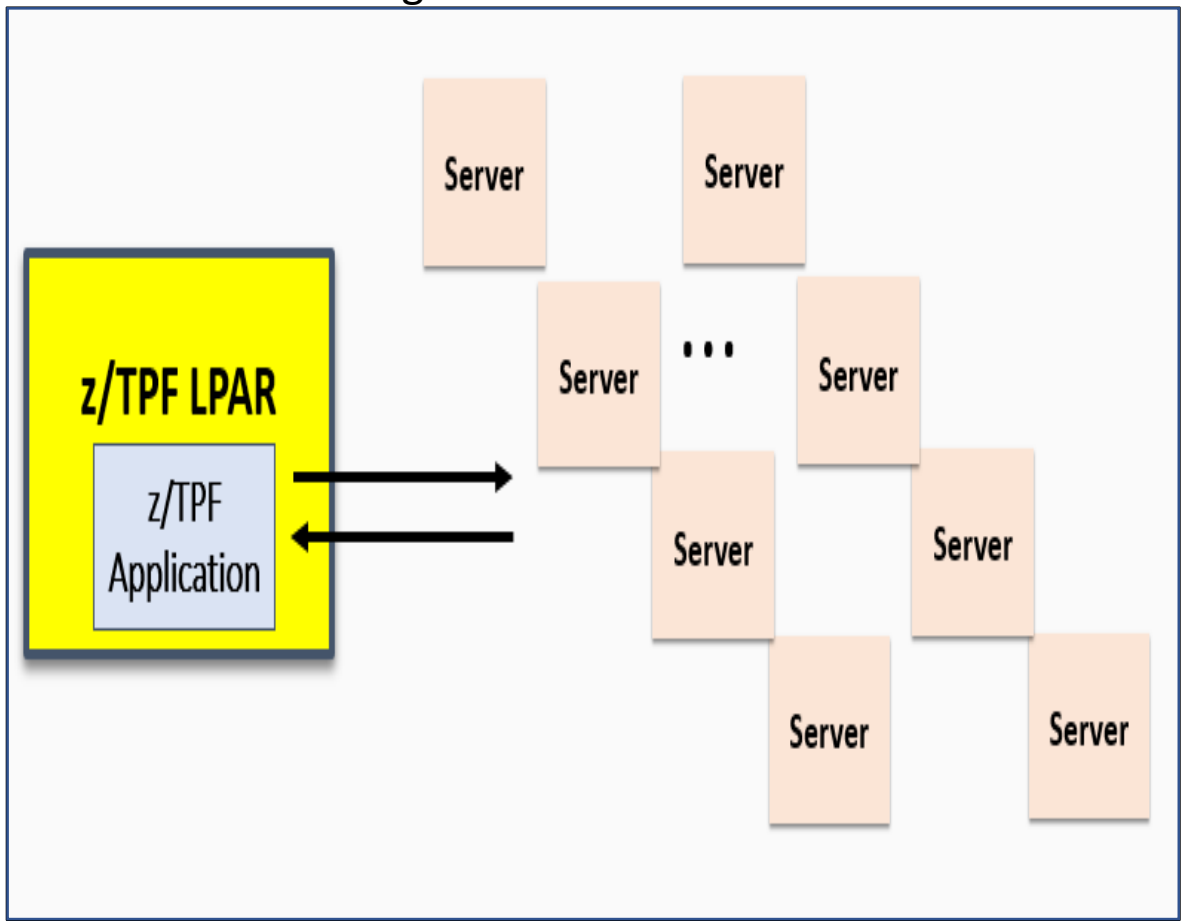
- Background
  - High Speed Connector
  - Enhanced HTTP Client
- Problem Statement
- Solution
  - Enabling z/TPF High Speed Connector, Enhanced HTTP Client and REST consumer for TLS.

Background – High Speed Connector Use Cases

Communicating with LPARs in Same CEC



Communicating with local or remote server farm



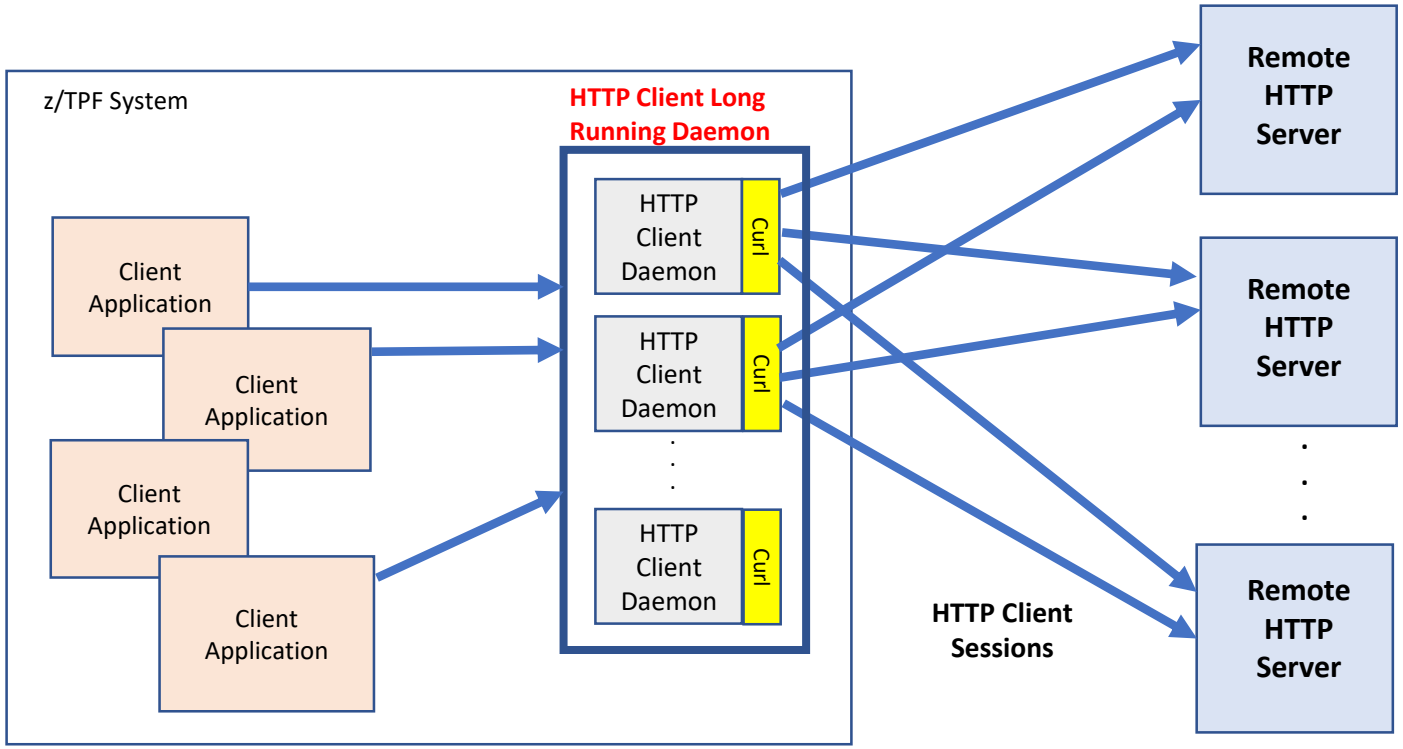
Background – High Speed Connector

- Administrator can define groups of servers
  - Defined through configuration
- The z/TPF system handles
  - Load balancing
  - Error handling and automatic session establishment
  - Statistics
  - Topology can be changed without affecting existing applications!

- Easier for applications to communicate with remote servers
  - Single API to send requests

- Delivered 3Q 2016, PUT 13 – APAR PJ43832
  - API for asynchronous responses delivered in Dec 2018 - PJ44733

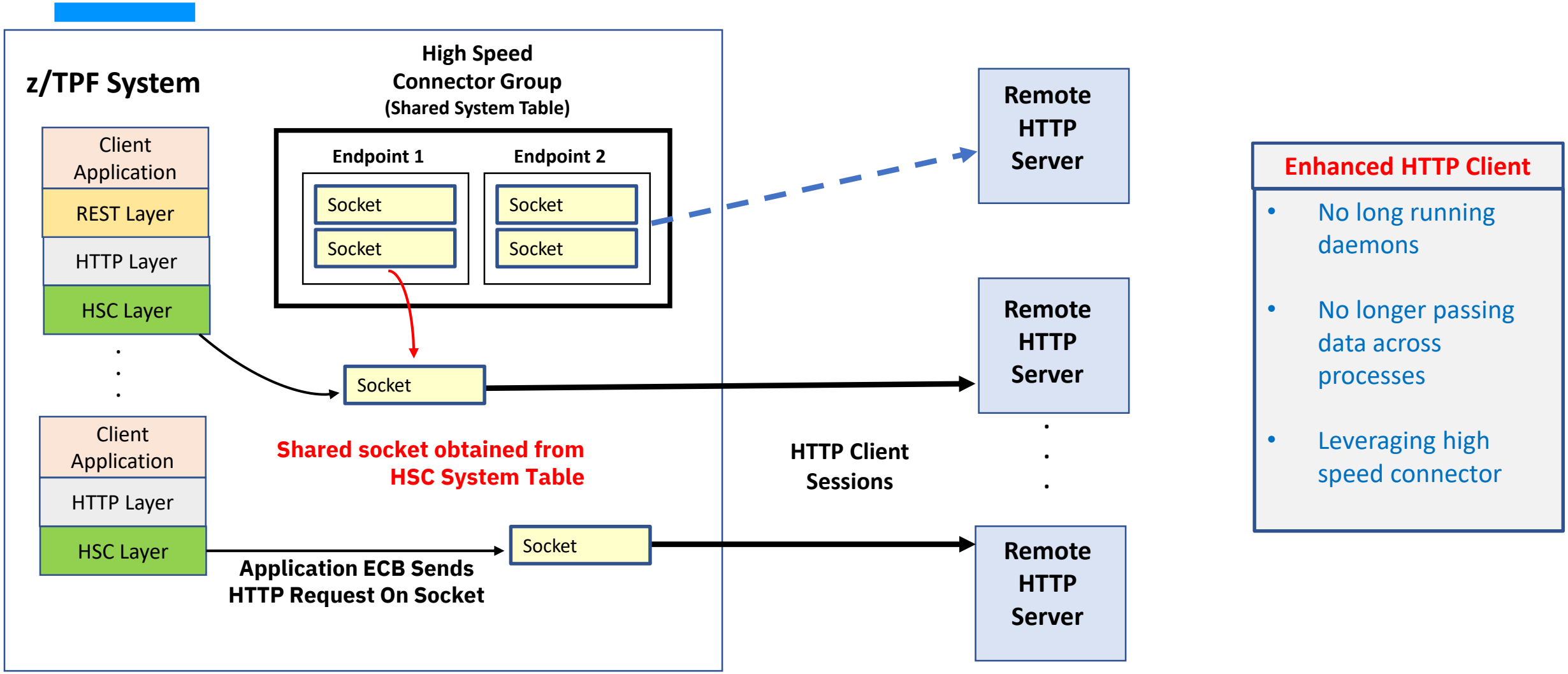
Background – Original HTTP Client



Original HTTP Client

- Long Running Daemons are not automatically recycled.
- Inefficient model to pass data across processes.
- Current libCurl package does not support the latest TLS standards.
- REST consumer would require significant changes to original HTTP client support

Background – Enhanced HTTP Client / REST Consumer



Enhanced HTTP Client

- No long running daemons
- No longer passing data across processes
- Leveraging high speed connector

Background – Enhanced HTTP Client / REST Consumer

- Delivered 4Q 2017, PUT 14 (PJ44733)
- Better performing HTTP client for z/TPF
  - Reduction of CPU usage in the HTTP layer up to 80%

- REST Consumer Support
  - Requires the Enhanced HTTP Client
  - Delivered 4Q 2017, PUT 14 (PJ45005)

- 100% TE-Eligible

Problem

- The High Speed Connector, Enhanced HTTP Client, or REST Consumer does not support Transport Layer Security (TLS)
  - Ability to communicate across secure sessions does not exist.

Example HTTP/REST Endpoint Configuration

```
<tns:EndpointGroup xmlns:tns="http://www.ibm.com/xmlns/prod/ztpf/endpoint"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.ibm.com/xmlns/prod/ztpf/endpoint /sys/tpf_pbfiles/tpf-
    fdes/schema/tpf_endpoint_schema.xsd ">
  <tns:Endpoint>
    <tns:endpointName>tpf1hts</tns:endpointName>
    <tns:role>PRIMARY</tns:role>
    <tns:destination>tpfLnx.pok.ibm.com1:71</tns:destination>
    <tns:startSocket>0</tns:startSocket>
    <tns:maxSocket>10</tns:maxSocket>
    <tns:bufferSendSize>1048576</tns:bufferSendSize>
    <tns:bufferReceiveSize>1048576</tns:bufferReceiveSize>
  </tns:Endpoint>
  <tns:groupName>tpfLnx</tns:groupName>
  <tns:groupType>HTTP</tns:groupType>
  <tns:TLS>YES</tns:TLS>
  <tns:groupDescription>Used to communicate with
       zLinux to getFlightInfo </tns:groupDescription>
  <tns:qMaxDepth>100</tns:qMaxDepth>
  <tns:qThreshold>80</tns:qThreshold>
  <tns:syncTimeout>3000</tns:syncTimeout>
  <tns:heartbeatInterval>0</tns:heartbeatInterval>
  <tns:aliasHostname>tpfLnx.pok.ibm.com</tns:aliasHostname>
  <tns:aliasHostname>tpfLnx.pok.ibm.com:71</tns:aliasHostname>
</tns:EndpointGroup>
```

One or more endpoint Definitions in group

Indicates Group is for HTTP/REST

Indicates Group is TLS

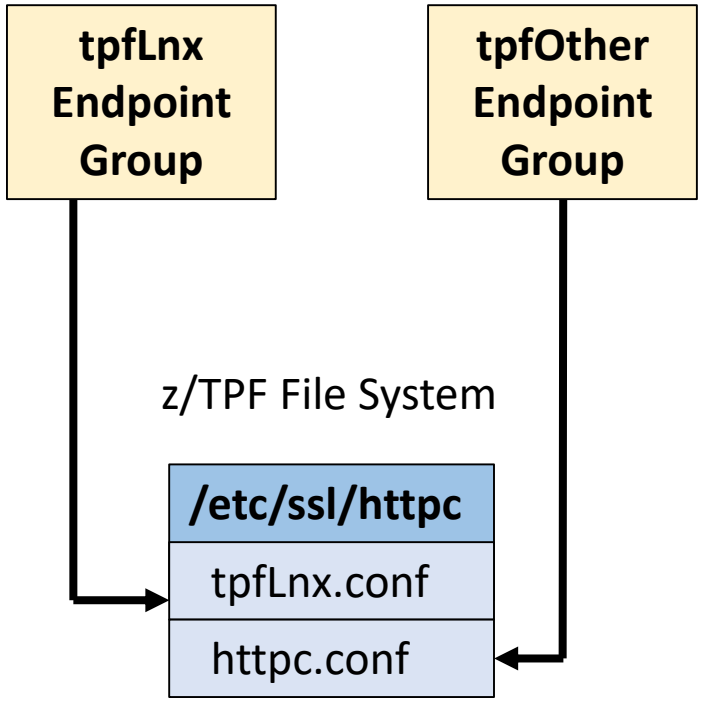
*z/TPF will look for TLS configuration

Hostnames associated with this group (Only valid for groupType:HTTP)

Enhanced HTTP Client - TLS Configuration Information

- If the endpoint configuration is for HTTP
  - The TLS HTTP client configuration file(s) reside in /etc/ssl/httpc/
  - Same location as original HTTP client for ease of migration

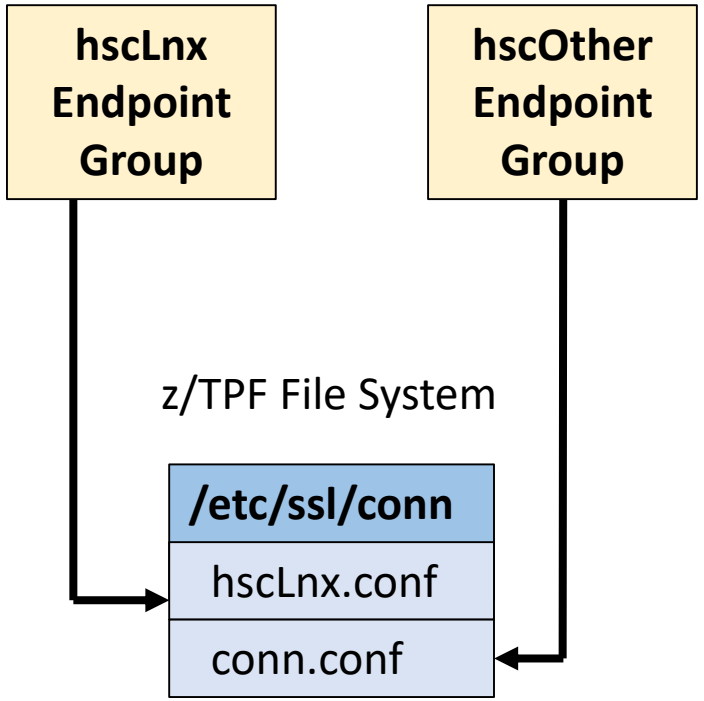
- Naming convention
  - *nnn*.conf : where *nnn* is the name of the HTTP endpoint group
  - httpc.conf can be coded as the default



High Speed Connector - TLS Configuration Information

- If the endpoint configuration is not for HTTP
  - The TLS HTTP client configuration file(s) reside in /etc/ssl/conn/

- Naming convention
  - *nnn*.conf : where *nnn* is the name of the high speed connector endpoint group
  - conn.conf can be coded as the default



Example TLS Configuration File

- Format of the TLS configuration file for High Speed Connector or Enhanced HTTP client is the same
  - Same configuration file format as MQ, INETD, etc.

```
VERSION=TLSv1_2
CIPHER=AES256-SHA256
VERIFYPEER=YES
CAINFO=/certs/cacert.pem
CERTIFICATE=/certs/ntpf2048_cert.pem
CERTTYPE=PEM
KEY=/tpfpubk/ntpf2048.pem
KEYTYPE=PEM
```

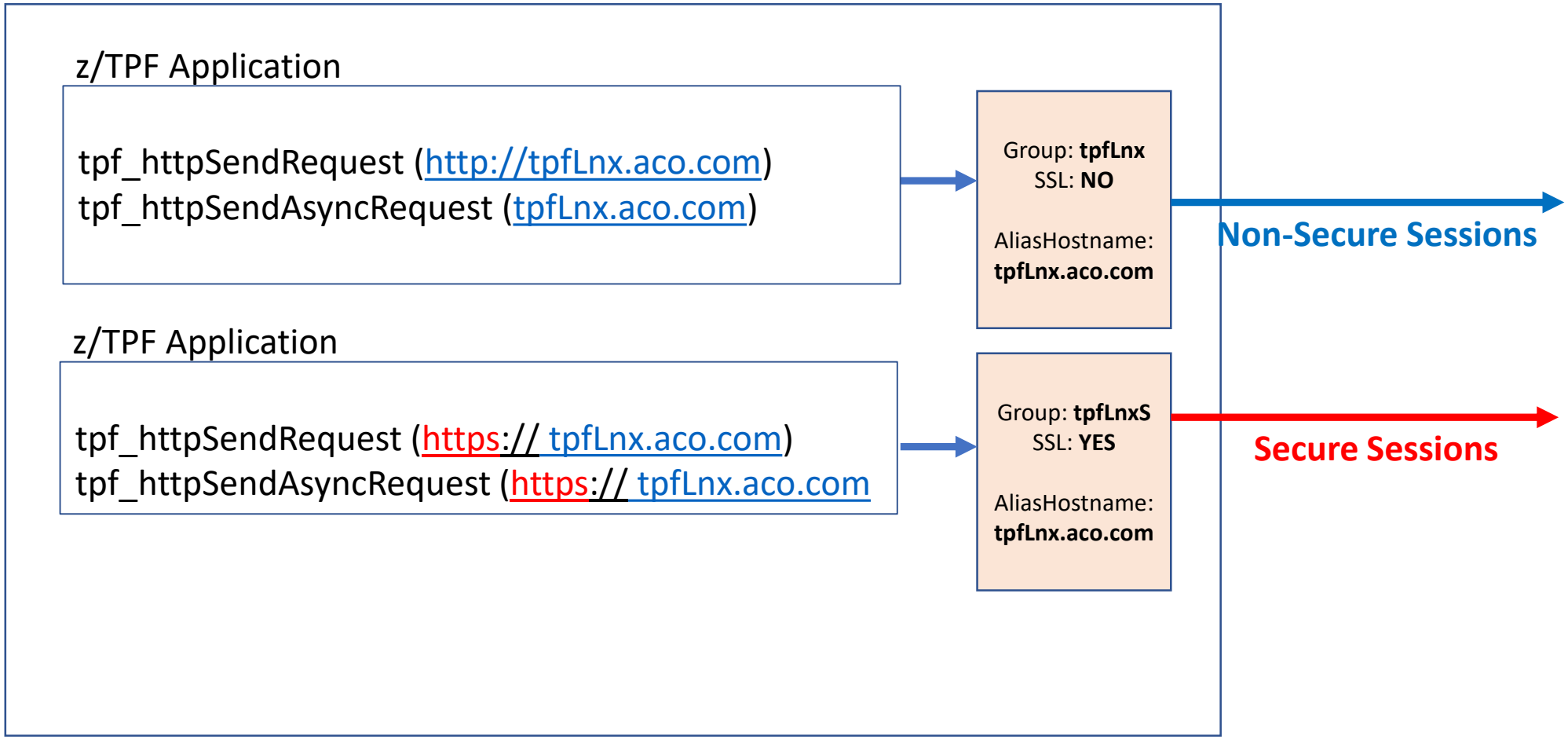
Required set of Parameters

Only required when server requests client authentication

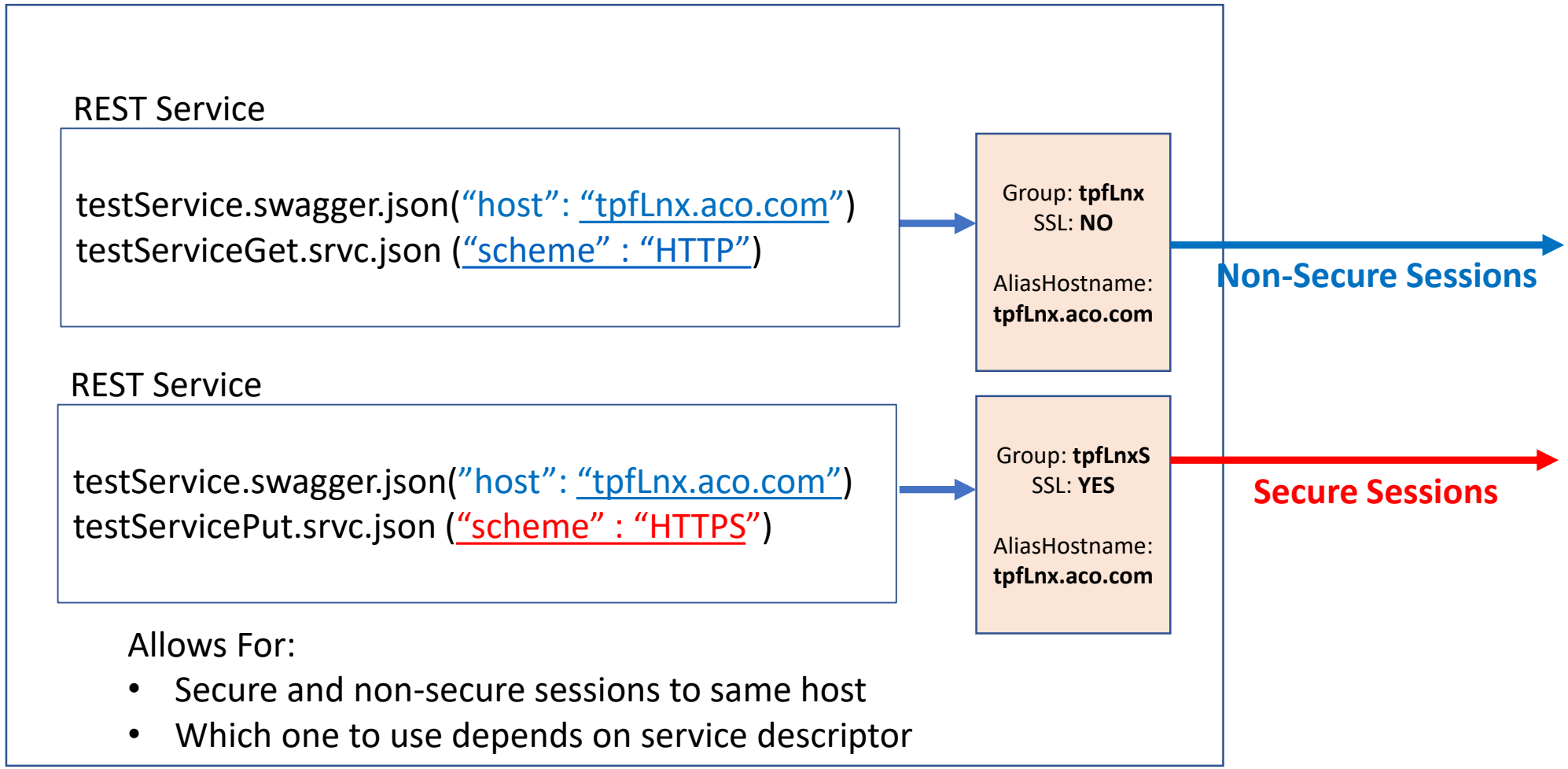
Enhanced HTTP Client: Non-Persistent Connections

- The enhanced HTTP Client provides the ability to send HTTP requests across a non-persistent HTTP client session.
  - If an endpoint group for the host specified by the application is not found
    - We create a session that will only remain active for the life of the application request.
    - Session is torn down upon receiving the response.
- Transport Layer Security for non-persistent HTTP client remains the same as the original HTTP Client
  - TLS configuration file in /etc/ssl/httpc must be names "*host*.conf", where *host* is the host the application is connecting to.
    - For example, airco.payment.com
  - If configuration file for host is not found, the default file httpc.conf is interrogated for the TLS configuration

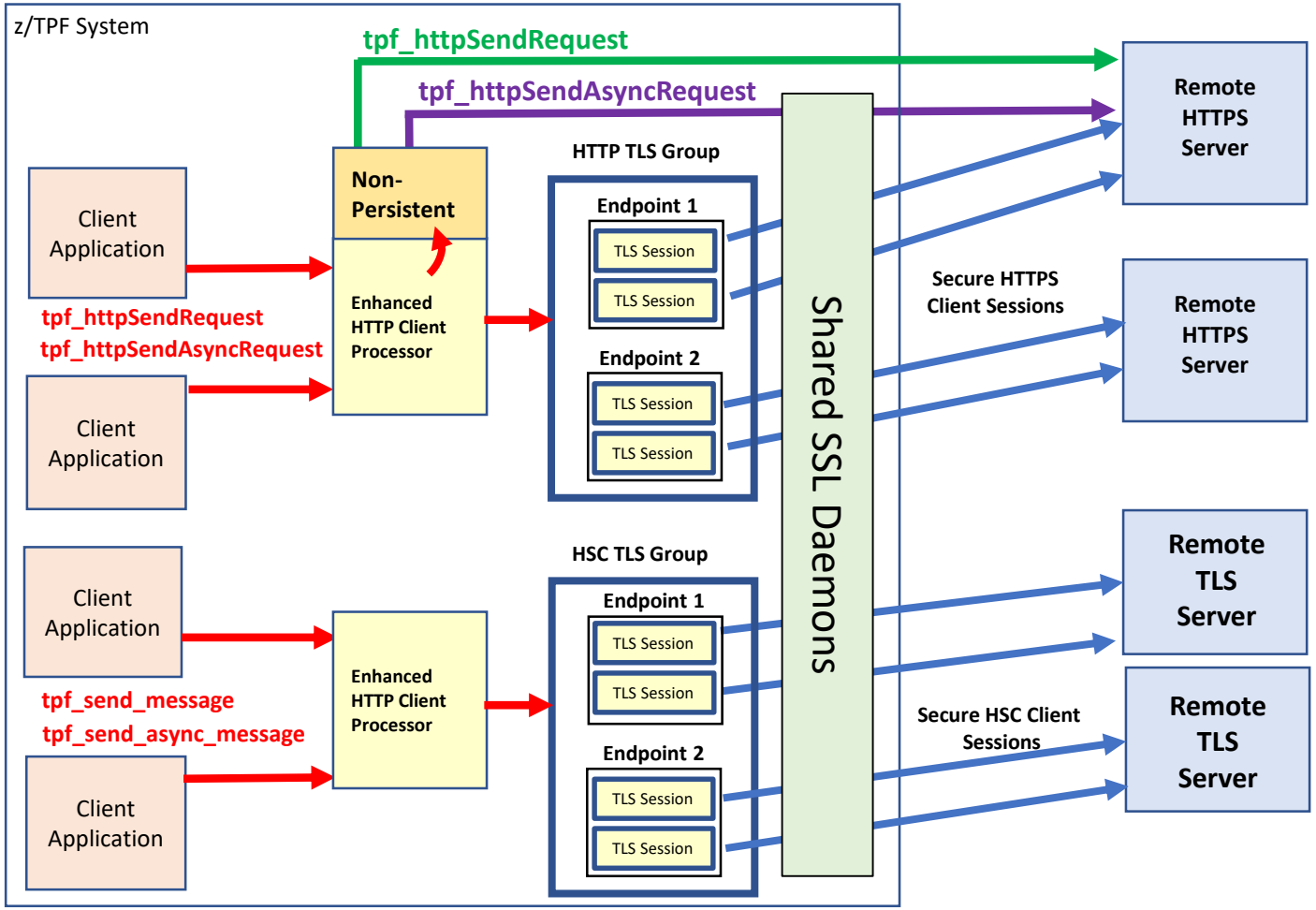
Remote Systems with SSL and non-SSL Servers



REST Consumer Layer



Enhanced HTTP and High Speed Connector TLS Architecture



- Architecturally TLS vs non-TLS is very similar
- The z/TPF Shared SSL Daemons are required for Enhanced HTTP or High Speed Connector across TLS.
  - Asynchronous API processing
  - Shared Sessions

Value Statement

- z/TPF system managed groups of SSL Sessions to remote servers.
  - Session establishment and management is handled by the z/TPF system

- Enables z/TPF applications to communicate with secure cloud based services.

Recap

- TLS Support for High Speed Connector, Enhanced HTTP Client, REST Consumer
  - PJ45258
  - Delivered October 2018, PUT 15
    - PJ45493 is a prerequisite (REST Consumer TLS Infrastructure)

Thank You!

Questions or Comments?

Trademarks

IBM, the IBM logo, ibm.com and Rational are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

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.