ERICSSON

Content Enrichment Configuration

OPERATION DIRECTIONS

17/1543-AXB 250 10/4-V3 Uen B

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.

Contents

1 Introduction

This document describes content enrichment configuration in the EPG.

1.1 Scope

This document covers the following issues:

— Configure content enrichment parameters

— Configure content enrichment rules

— Associate content enrichment rules

For an overview of content enrichment, refer to Content Enrichment.

1.2 Target Groups

This document is intended for personnel performing configuration of the EPG. The document assumes a basic knowledge of data communication and telecommunication.

2 Activate Licensed Features

Optional licensed features in the EPG are turned off by default. To employ these features in the EPG, licenses must be purchased from Ericsson. For information on how to purchase licenses and enable licensed features, refer to Software License Management or contact your local Ericsson support.

To enable content enrichment, activate the Content Enrichment: Header Editing license.

3 Configure Content Enrichment Parameters

3.1 Configure RAT Type Parameter

The inserted value for RAT type can be textual instead of numerical. To configure the mapping between a numerical RAT type and a textual value, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name> edit
-content rat-type map <rat-type-text>
   id <rat-type-id>
```

Note: The configuration applies to all HTTP and TLS content enrichment rules inside the rule space.

3.2 Configure Roaming Status Parameter

The inserted value for the roaming status is derived from roaming detection by comparing the serving PLMN ID of a user session, or the serving node address mapped to the PLMN, with the PLMN ID of the GGSN or PGW.

— The PLMN ID of the GGSN or PGW must be configured. For information on how to configure the PLMN ID of the GGSN or PGW, refer to APN Configuration.

— The serving PLMN ID is included in the PDP context request message. If not, the serving node address mapped to the PLMN can be used. For information on how to map serving node addresses to PLMNs, refer to APN Configuration.

4 Content Enrichment Rules

Content can be inserted as protocol headers, extensions, or body content, depending on the protocol. A content enrichment rule consists of a set of items, one per piece of content to be inserted. Items are defined within the named header or extension to be inserted, if applicable. Each item consists of the textual key, the parameter, and a separator inbetween, to be contained in the item. The default separator between an inserted pair of key and parameter is set to an equal sign (=). The default separator between inserted items is set to a space ( ). Optionally, the separator between the key and the parameter, and between inserted items, can be configured as a set of characters, or disabled by configuring an empty separator ("").

In addition, a content enrichment rule can contain the name of an original header, to invalidate that specific header.

When configuring HTTP or SSL/TLS content enrichment, any changes made to the content enrichment configuration only affect new user sessions immediately. Existing user sessions are affected too, but do not contain the new session parameters if any were added in the configuration. For existing user sessions to get all the new enriched session parameters, the user session must be deleted and recreated.

When configuring IMAP or SMTP content enrichment, existing user sessions are affected too, but do not contain the new session parameters if any were added in the configuration. For existing user sessions to get all the new enriched session parameters, the user session must be deleted and recreated.

Table 1 shows which characters can be used for content enrichment.

Table 1 Allowed Characters for Content Enrichment

Allowed characters		
Header name and header content	Encryption key	Separator
0–9, A-Z, a-z	0–9, A-Z, a-z, -, ., _	0–9, A-Z, a-z, !, #, $, *, +, -, ., /, :, >, =, ? (with quotation marks around ("?")), @, ~, _

5 Configure Content Enrichment

5.1 Configure HTTP Content Enrichment

To perform HTTP content enrichment, do the following:

1. Configure an HTTP content enrichment rule, see Section 6.1 on page 5 and Section 6.2 on page 12.

2. Associate an ACR or an HTTP-WSP rule with the HTTP content enrichment rule, see Section 7.1 on page 20.

After performing the steps of HTTP content enrichment configuration, the node configuration resembles the examples in Section 6.1 on page 5 and Section 7.1 on page 20.

5.2 Configure IMAP Content Enrichment

To perform IMAP content enrichment, do the following:

1. Configure an IMAP content enrichment rule, see Section 6.3 on page 13.
2. Associate a content enrichment rule with the IMAP content enrichment rule, see Section 7.2 on page 21.

After performing the steps of IMAP content enrichment configuration, the node configuration resembles the examples in Section 6.3 on page 13 and Section 7.2 on page 21.

5.3 Configure SMTP Content Enrichment

To perform SMTP content enrichment, do the following:

1. Configure an SMTP content enrichment rule, see Section 6.4 on page 14.
2. Associate a content enrichment rule with the SMTP content enrichment rule, see Section 7.3 on page 21.

After performing the steps of SMTP content enrichment configuration, the node configuration resembles the examples in Section 6.4 on page 14 and Section 7.3 on page 21.

5.4 Configure SSL/TLS Content Enrichment

To perform SSL/TLS content enrichment, do the following:

1. Configure an SSL/TLS content enrichment rule, see Section 6.5 on page 15 and Section 6.6 on page 18.
2. Associate an ACR or a content enrichment rule with the SSL/TLS content enrichment rule, see Section 7.4 on page 22.

After performing the steps of SSL/TLS content enrichment configuration, the node configuration resembles the examples in Section 6.5 on page 15 and Section 7.4 on page 22.

6 Configure Content Enrichment Rules

The following two content enrichment configuration rules exist:

— ACR-based content enrichment rule

— PISC-based content enrichment rule

Any content enrichment rules can be selected, but it is recommended to update the configuration files and use the ACR-based content enrichment rule, however it is not mandatory.

If both configuration rules can be applied for a packet, PISC-based content enrichment rule has priority.

6.1 Configure HTTP Header Enrichment Rules

The extended headers in the HTTP header and the items within a single extended header are placed in the order they are entered in the Command Line Interface (CLI).

The following applies to ACR-based HTTP header enrichment rules:

— If the header is encrypted, all items are encrypted.

— Maximum 8 items can be added into the header.

— Non-encrypted items can be concatenated with encrypted items.

— When an item contains a subitem, parameters and keys cannot be configured within that item.

— Maximum 8 subitems can be added into an item.

The following applies to PISC-based HTTP header enrichment rules:

— Maximum 4 items can be added into the header.

— The separator between items or between key and parameter cannot be disabled.

— All items within the header are encrypted with the algorithm configured.

— Non-encrypted items cannot be concatenated with encrypted items.

— Subitems cannot be configured.

6.1.1 Configure an HTTP Header

A header consists of a header name and one or more items, see Section 6.1.2 on page 7, with separators inbetween. Header contents can be encrypted using a specific pre-shared key or certificate, see Section 6.1.4 on page 10.

6.1.1.1 Configure an HTTP Header Separator

To configure an HTTP header enrichment rule to insert a separator between inserted items, include the following statement:

— **ACR-based:**

```
Ericsson(config)# epg pgw service-identification content-enrich
ment-rule <rule-name> http insert extended-header <header-name>
   separator <separator>
```

— **PISC-based:**

```
Ericsson(config)# epg pgw service-identification http-wsp-edit
-rule <rule-name> insert extended-header <header-name>
   separator <separator>
```

6.1.1.2 Configure an HTTP Header RC4 Encryption

To configure an HTTP header enrichment rule to activate RC4 encryption, as per Section 6.1.4.1 on page 10, for the header contents, include the following statement:

— **ACR-based:**

```
Ericsson(config)# epg pgw service-identification content-enrich
ment-rule <rule-name> http insert extended-header <header-name>
   encrypt rc4
```

6.1.1.3 Configure an HTTP Header RC4-MD5 Encryption

To configure an HTTP header enrichment rule to activate RC4-MD5 encryption, as per Section 6.1.4.2 on page 10, for the header contents, include the following statement:

— **ACR-based:**

```
Ericsson(config)# epg pgw service-identification content-enrich
ment-rule <rule-name> http insert extended-header <header-name>
   encrypt rc4-md5
```

6.1.1.4 Configure an HTTP Header RSA Encryption

To configure an HTTP header enrichment rule to activate RSA encryption, as per Section 6.1.4.3 on page 10, for the header contents, include the following statement:

— **ACR-based:**

```
Ericsson(config)# epg pgw service-identification content-enrich
ment-rule <rule-name> http insert extended-header <header-name>
```

```
encrypt rsa
```

6.1.2 Configure an HTTP Item

An item consists of a key and/or a parameter with a separator inbetween, alternatively one or more subitems with separators inbetween, see Section 6.1.3 on page 9. Item contents can be encrypted using a specific pre-shared key or certificate, see Section 6.1.4 on page 10.

6.1.2.1 Configure an HTTP Item Key

To configure an HTTP header enrichment rule to insert an item containing a key, include the following statement:

— **ACR-based:**

```
Ericsson(config)# epg pgw service-identification content
-enrichment-rule <rule-name> http insert extended-header
<header-name> item <item-id>
   key <key-value>
```

— **PISC-based:**

```
ex
Ericsson(config)# epg pgw service-identification http
-wsp-edit-rule <rule-name> insert extended-header
<header-name> item <item-id>
   key <key-value>
```

6.1.2.2 Configure an HTTP Item Parameter

To configure an HTTP header enrichment rule to insert an item containing a parameter, include the following statement:

— **ACR-based:**

```
Ericsson(config)# epg pgw service-identification content
-enrichment-rule <rule-name> http insert extended-header
<header-name> item <item-id>
   parameter (apn | auth-acg | cc | cid | cust-id |
ggsn-pgw-ip | imei | imsi | msisdn | msisdn-no-cc |
packet-dateandtime-epoch | packet-dateandtime-iso | plmn-id |
rat-type | roaming | serving-node-ip | session-dateandtime-iso
| time-zone | ue-ip | uli | unauth-acg)
```

— **PISC-based:**

```
Ericsson(config)# epg pgw service-identification http
-wsp-edit-rule <rule-name> insert extended-header
<header-name> item <item-id>
```

```
   parameter (apn | auth-acg | cc | cid | cust-id |
ggsn-pgw-ip | imei | imsi | msisdn | msisdn-no-cc |
plmn-id | rat-type | roaming | serving-node-ip | time-zone
| ue-ip | uli | unauth-acg)
```

6.1.2.3 Configure an HTTP Item Separator

To configure an HTTP header enrichment rule to insert an item containing a separator between inserted key and parameter or subitems, include the following statement:

— **ACR-based:**

```
Ericsson(config)# epg pgw service-identification content
-enrichment-rule <rule-name> http insert extended-header
<header-name> item <item-id>
   separator <separator>
```

— **PISC-based:**

```
Ericsson(config)# epg pgw service-identification http
-wsp-edit-rule <rule-name> insert extended-header
<header-name> item <item-id>
   separator <separator>
```

6.1.2.4 Configure an HTTP Item RC4 Encryption

To configure an HTTP header enrichment rule to activate RC4 encryption, as per Section 6.1.4.1 on page 10, for the item contents, include the following statement:

— **ACR-based:**

```
Ericsson(config)# epg pgw service-identification content
-enrichment-rule <rule-name> http insert extended-header
<header-name> item <item-id>
   encrypt rc4
```

6.1.2.5 Configure an HTTP Item RC4-MD5 Encryption

To configure an HTTP header enrichment rule to activate RC4-MD5 encryption, as per Section 6.1.4.2 on page 10, for the item contents, include the following statement:

— **ACR-based:**

```
Ericsson(config)# epg pgw service-identification content
-enrichment-rule <rule-name> http insert extended-header
<header-name> item <item-id>
   encrypt rc4-md5
```

6.1.2.6 Configure an HTTP Item RSA Encryption

To configure an HTTP header enrichment rule to activate RSA encryption, as per Section 6.1.4.3 on page 10, for the item contents, include the following statement:

— **ACR-based:**

```
Ericsson(config)# epg pgw service-identification content
-enrichment-rule <rule-name> http insert extended-header
<header-name> item <item-id>
   encrypt rsa
```

6.1.3 Configure an HTTP Subitem

A subitem consists of a key and/or a parameter with a separator inbetween.

6.1.3.1 Configure an HTTP Subitem Key

To configure an HTTP header enrichment rule to insert a subitem containing a key, include the following statement:

— **ACR-based:**

```
Ericsson(config)# epg pgw service-identification content
-enrichment-rule <rule-name> http insert extended-header
<header-name> item <item-id> item <subitem-id>
   key <key>
```

6.1.3.2 Configure an HTTP Subitem Parameter

To configure an HTTP header enrichment rule to insert a subitem containing a parameter, include the following statement:

— **ACR-based:**

```
Ericsson(config)# epg pgw service-identification content
-enrichment-rule <rule-name> http insert extended-header
<header-name> item <item-id> item <subitem-id>
   parameter (apn | auth-acg | cc | cid | cust-id |
ggsn-pgw-ip | imei | imsi | msisdn | msisdn-no-cc |
packet-dateandtime-epoch | packet-dateandtime-iso | plmn-id |
rat-type | roaming | serving-node-ip | session-dateandtime-iso
| time-zone | ue-ip | uli | unauth-acg)
```

6.1.3.3 Configure an HTTP Subitem Separator

To configure an HTTP header enrichment rule to insert a subitem containing a separator between inserted key and parameter, include the following statement:

— **ACR-based:**

```
Ericsson(config)# epg pgw service-identification content
-enrichment-rule <rule-name> http insert extended-header
<header-name> item <item-id> item <subitem-id>
   separator <separator>
```

6.1.4 Configure an HTTP Encryption

6.1.4.1 Configure RC4 Secret

To configure an HTTP header enrichment rule to use RC4 encryption, include the following statement:

— **ACR-based:**

```
Ericsson(config)# epg pgw service-identification content
-enrichment-rule <rule-name> http insert extended-header
<header-name> rc4-encryption
   pre-shared-key-clear <key-value>
```

— **PISC-based:**

```
Ericsson(config)# epg pgw service-identification http-wsp-edit
-rule <rule-name> insert extended-header <header-name>
   secret-clear <key-value>
```

6.1.4.2 Configure RC4-MD5 Secret

To configure an HTTP header enrichment rule to use RC4-MD5 encryption, include the following statement:

— **ACR-based:**

```
Ericsson(config)# epg pgw service-identification content
-enrichment-rule <rule-name> http insert extended-header
<header-name> rc4-md5-encryption
   pre-shared-key <key-value>
```

— **PISC-based:**

```
Ericsson(config)# epg pgw service-identification http-wsp-edit
-rule <rule-name> insert extended-header <header-name>
   secret <key-value>
```

6.1.4.3 Configure RSA Certificate

To configure an HTTP header enrichment rule to use RSA encryption, include the following statement:

— **ACR-based:**

To configure RSA encryption using the public key in a node credential or trusted certificate object, include the following statement:

```
Ericsson(config)# epg pgw service-identification content
-enrichment-rule <rule-name> http insert extended-header
<header-name> rsa-encryption
   certificate <key-value>
```

To configure RSA encryption using the public key in a trusted certificate object, the trust category to which the trusted certificate belongs, must be configured. To configure the trust category, include the following statement:

```
Ericsson(config)# epg pgw service-identification content
-enrichment-rule <rule-name> http insert extended-header
<header-name> rsa-encryption
   trust-category <name>
```

Note: To configure RSA encryption based on a trusted certificate, the certificate name and the trust category name must be the same. For more information about certificates, refer to Certificate Management.

6.1.5 Examples of HTTP Header Enrichment and Header Override Rules

After performing the configuration of the ACR-based HTTP header enrichment rules, the node configuration resembles Example 1.

```
epg pgw service-identification content-enrichment-rule insert-cid
 http insert extended-header x-msisdn1
  item ggsn-pgw-ip
   key       ggsn-pgw-ip
   separator -
   parameter ggsn-pgw-ip
  !
  item msisdn
   key       msisdn
   separator -
   parameter msisdn
  !
 !
 http insert extended-header x-msisdn2
  secret "$8$13ya4tyuQ7NKIr5FkDjknBV0C6ntoX9gXHX5Sf4NCuGtGLdPPsu4UE2p1kJg59tHigfJtlyR\nF6+BKzbW
  item ggsn-pgw-ip
   key       ggsn-pgw-ip
   separator -
   parameter ggsn-pgw-ip
  !
  item msisdn
   key       msisdn
   separator -
   parameter msisdn
  !
 !
 http insert extended-header x-msisdn3
  item msisdn
   parameter msisdn
  !
 !
 http invalidate extended-header x-msisdn1
 http invalidate extended-header x-msisdn2
 !
!
```

Example 1 HTTP Header Enrichment and Header Override Rule Configuration Example

After performing the configuration of the PISC-based HTTP header enrichment rules, the node configuration resembles Example 2.

```
epg pgw service-identification http-wsp-edit-rule insert-cid
 insert extended-header x-msisdn1
  item ggsn-pgw-ip
   key       ggsn-pgw-ip
   separator -
   parameter ggsn-pgw-ip
  !
  item msisdn
   key       msisdn
   separator -
   parameter msisdn
  !
 !
 insert extended-header x-msisdn2
  secret "$8$s6G5OeBtxX16bZZLRmL6omyv5aa4wt0xJvbEu+BUeP09sCaqsinas/nyWPusB/ecQdlydycL\nhsNf7u5tRA0
  item ggsn-pgw-ip
   key       ggsn-pgw-ip
   separator -
   parameter ggsn-pgw-ip
  !
  item msisdn
   key       msisdn
   separator -
   parameter msisdn
  !
 !
 insert extended-header x-msisdn3
  item msisdn
   parameter msisdn
  !
 !
 invalidate extended-header x-msisdn4
 !
!
```

Example 2 HTTP Header Enrichment and Header Override Rule Configuration Example

6.2 Configure HTTP Header Override Rules

To configure an HTTP header override rule, include the following statement:

— **ACR-based:**

```
Ericsson(config)# epg pgw service-identification content-e
nrichment-rule <rule-name> http invalidate
   extended-header <header-name>
```

Up to 20 HTTP headers can be configured for override in a given header override rule.

After performing the configuration of the ACR-based HTTP header override rules, the node configuration resembles Example 1.

— **PISC-based:**

```
Ericsson(config)# epg pgw service-identification http-w
sp-edit-rule <rule-name> invalidate
   extended-header <header-name>
```

Only one HTTP header can be configured for override in a given header override rule.

After performing the configuration of the PISC-based HTTP header override rules, the node configuration resembles Example 2.

6.3 Configure IMAP Content Enrichment Rules

6.3.1 Configure IMAP Content Separator

To configure an IMAP content enrichment rule to insert a separator between inserted content, include the following statement:

— **PISC-based:**

```
Ericsson(config)# epg pgw service-identification imap
-edit-rule <rule-name> insert
   separator <separator>
```

6.3.2 Configure an IMAP Item

6.3.2.1 Configure an IMAP Item Key

To configure an IMAP content enrichment rule to insert a key, include the following statement:

— **PISC-based:**

```
Ericsson(config)# epg pgw service-identification imap-edit-rule
<rule-name> insert item <item-id>
   key <key>
```

6.3.2.2 Configure an IMAP Item Parameter

To configure an IMAP content enrichment rule to insert a parameter, include the following statement:

— **PISC-based:**

```
Ericsson(config)# epg pgw service-identification imap-edit-rule
<rule-name> insert item <item-id>
   parameter (cc | cid | ggsn-pgw-ip | imei | imsi | msisdn
| msisdn-no-cc | serving-node-ip | ue-ip)
```

6.3.2.3 Configure an IMAP Item Separator

To configure an IMAP content enrichment rule to insert a separator between inserted key and parameter, include the following statement:

— **PISC-based:**

```
Ericsson(config)# epg pgw service-identification imap-edit-rule
<rule-name> insert item <item-id>
   separator <separator>
```

6.3.3 Examples of IMAP Content Enrichment Rules

After performing the configuration of the PISC-based IMAP content enrichment rules, the node configuration resembles Example 3.

```
epg pgw service-identification imap-edit-rule insert-cid
 insert item ggsn-pgw-ip
  key       ggsn-pgw-ip
  separator -
  parameter ggsn-pgw-ip
 !
 insert item msisdn
  key       msisdn
  separator -
  parameter msisdn
 !
!
```

Example 3 IMAP Content Enrichment Rule Configuration Example

6.4 Configure SMTP Content Enrichment Rules

6.4.1 Configure SMTP Content Separator

To configure an SMTP content enrichment rule to insert a separator between inserted content, include the following statement:

— **PISC-based:**

```
Ericsson(config)# epg pgw service-identification smtp
-edit-rule <rule-name> insert
   separator <separator>
```

6.4.2 Configure an SMTP Item

6.4.2.1 Configure an SMTP Item Key

To configure an SMTP content enrichment rule to insert a key, include the following statement:

— **PISC-based**

```
Ericsson(config)# epg pgw service-identification smtp-edit-rule
<rule-name> insert item <item-id>
   key <key>
```

6.4.2.2 Configure an SMTP Item Parameter

To configure an SMTP content enrichment rule to insert a parameter, include the following statement:

— **PISC-based:**

```
Ericsson(config)# epg pgw service-identification smtp-edit-rule
<rule-name> insert item <item-id>
   parameter (cc | cid | ggsn-pgw-ip | imei | imsi | msisdn
| msisdn-no-cc | serving-node-ip | ue-ip)
```

6.4.2.3 Configure an SMTP Item Separator

To configure an SMTP content enrichment rule to insert a separator between inserted key and parameter, include the following statement:

— **PISC-based:**

```
Ericsson(config)# epg pgw service-identification smtp-edit-rule
<rule-name> insert item <item-id>
   separator <separator>
```

6.4.3 Examples of SMTP Content Enrichment Rules

After performing the configuration of the PISC-based SMTP content enrichment rules, the node configuration resembles Example 4.

```
epg pgw service-identification smtp-edit-rule insert-cid
 insert item ggsn-pgw-ip
  key       ggsn-pgw-ip
  separator -
  parameter ggsn-pgw-ip
 !
 insert item msisdn
  key       msisdn
  separator -
  parameter msisdn
 !
!
```

Example 4 SMTP Content Enrichment Rule Configuration Example

6.5 Configure SSL/TLS Extension Enrichment Rules

6.5.1 Configure an SSL/TLS Extension

To configure an SSL/TLS extension enrichment rule to insert an extension, include the following statement:

— **ACR-based:**

```
Ericsson(config)# epg pgw service-identification content-e
nrichment-rule <rule-name> ssl-tls insert
   extension-number <value>
```

— **PISC-based:**

```
Ericsson(config)# epg pgw service-identification ssl-t
ls-edit-rule <rule-name> insert
   extension-number <value>
```

6.5.2 Configure an SSL/TLS Item

6.5.2.1 Configure an SSL/TLS Item Type

To configure an SSL/TLS extension enrichment rule to insert an item containing a type, include the following statement:

— **ACR-based:**

```
Ericsson(config)# epg pgw service-identification content-enr
ichment-rule <rule-name> ssl-tls insert item <item-id>
   type <type>
```

— **PISC-based**

```
Ericsson(config)# epg pgw service-identification ssl-tls-e
dit-rule <rule-name> insert item <item-id>
   type <type>
```

6.5.2.2 Configure an SSL/TLS Item Format

To configure an SSL/TLS extension enrichment rule to insert an item containing a format, include the following statement:

— **ACR-based:**

```
Ericsson(config)# epg pgw service-identification content-enr
ichment-rule <rule-name> ssl-tls insert item <item-id>
   format (binary | string)
```

— **PISC-based:**

```
Ericsson(config)# epg pgw service-identification ssl-tls-e
dit-rule <rule-name> insert item <item-id>
   format (binary | string)
```

6.5.2.3 Configure an SSL/TLS Item Parameter

To configure an SSL/TLS extension enrichment rule to insert an item containing a parameter, include the following statement:

— **ACR-based:**

```
Ericsson(config)# epg pgw service-identification content-enr
ichment-rule <rule-name> ssl-tls insert item <item-id>
   parameter (msisdn | ue-ip | serving-node-ip | ggsn-pgw-ip
| imsi | imei | auth-acg | cc | plmn-id | unauth-acg | uli |
rat-type | roaming | time-zone | apn | timestamp)
```

— **PISC-based:**

```
Ericsson(config)# epg pgw service-identification ssl-tls-e
dit-rule <rule-name> insert item <item-id>
   parameter (msisdn | ue-ip | serving-node-ip | ggsn-pgw-ip
| imsi | imei | auth-acg | cc | plmn-id | unauth-acg | uli |
rat-type | roaming | time-zone | apn | timestamp)
```

6.5.2.4 Configure an SSL/TLS Item Priority

To configure an SSL/TLS extension enrichment rule to insert an item containing priority, include the following statement:

— **ACR-based:**

```
Ericsson(config)# epg pgw service-identification content-enr
ichment-rule <rule-name> ssl-tls insert item <item-id>
   priority <priority>
```

— **PISC-based:**

```
Ericsson(config)# epg pgw service-identification ssl-tls-e
dit-rule <rule-name> insert item <item-id>
   priority <priority>
```

6.5.2.5 Configure an SSL/TLS Item Encryption

To configure an SSL/TLS extension enrichment rule to encrypt the inserted extensions using a `secret`, include the following statement:

Note: When `secret` is configured, only string values can be encrypted. Binary format cannot be used when encryption is configured.

— **ACR-based:**

```
Ericsson(config)# epg pgw service-identification content-enr
ichment-rule <rule-name> ssl-tls insert item <item-id>
   secret <key-value>
```

— **PISC-based:**

```
Ericsson(config)# epg pgw service-identification ssl-tls-e
dit-rule <rule-name> insert item <item-id>
   secret <key-value>
```

6.5.3 Examples of SSL/TLS Extension Enrichment and Override Rules

After performing the configuration of the ACR-based SSL/TLS extension enrichment rules, the node configuration resembles Example 5.

```
epg pgw service-identification content-enrichment-rule ce-01
 ssl-tls invalidate extension-number 1111
 ssl-tls invalidate new-extension-number 1112
 ssl-tls insert extension-number 1112
 ssl-tls insert item 1
  type      1
  priority  500
  format    binary
  parameter msisdn
 !
!
```

Example 5 Configuration Example of TLS Extension Enrichment and Override: Invalidate=1,newExtensionNumber equal to Insert=1,extensionNumber

After performing the configuration of the PISC-based SSL/TLS extension enrichment rules, the node configuration resembles Example 6.

```
epg pgw service-identification ssl-tls-edit-rule ce-01
 invalidate extension-number 1111
 invalidate new-extension-number 1112
 insert extension-number 1112
 insert item 1
  type      1
  priority  500
  format    binary
  parameter msisdn
 !
!
```

Example 6 Configuration Example of TLS Extension Enrichment and Override: Invalidate=1,newExtensionNumber equal to Insert=1,extensionNumber

6.6 Configure SSL/TLS Extension Override Rules

`extension-number` specifies the number corresponding to the extension type to be replaced.

`new-extension-number` specifies the number corresponding to the new extension type.

When configuring the extension override rule for TLS extension override, consider the following:

— `new-extension-number` must be different from `extension-number`.

— `new-extension-number` and `extension-number` are configured as decimals. The converted hexadecimal for `new-extension-number` must have the same highest order byte as that for `extension-number`.

  For example, the following configuration is valid:
  ```
  extension-number=65535 // 0xFFFF (HEX)
  new-extension-number=4092 // 0xFFC (HEX)
  ```

— A parameter cannot be configured more than once in the same extension override rule.

To configure an SSL/TLS extension override rule, include the following statement:

— **ACR-based:**

  ```
  Ericsson(config)# epg pgw service-identification content-e
  nrichment-rule <rule-name> ssl-tls invalidate
     extension-number <extension-number>
  Ericsson(config)# epg pgw service-identification content-e
  nrichment-rule <rule-name> ssl-tls invalidate
     new-extension-number <new-extension-number>
  ```

  After performing the configuration of the ACR-based SSL/TLS extension override rules, the node configuration resembles Example 5.

— **PISC-based:**

  ```
  Ericsson(config)# epg pgw service-identification ssl-t
  ls-edit-rule <rule-name> invalidate
     extension-number <extension-number>
  Ericsson(config)# epg pgw service-identification ssl-t
  ls-edit-rule <rule-name> invalidate
     new-extension-number <new-extension-number>
  ```

  After performing the configuration of the PISC-based SSL/TLS extension override rules, the node configuration resembles Example 6.

7 Associate Content Enrichment Rules

The following two content enrichment configuration rules exist:

— ACR-based content enrichment rule

— PISC-based content enrichment rule

Any content enrichment rules can be selected, but it is recommended to update the configuration files and use the ACR-based content enrichment rule, however it is not mandatory.

If both configuration rules can be applied for a packet, PISC-based content enrichment rule has priority.

7.1 Associate HTTP Content Enrichment Rules

If a packet is successfully matched to an HTTP-WSP rule and the HTTP-WSP rule term is associated with a content enrichment rule, the EPG applies all the header enrichment actions configured for the associated content enrichment rule.

Associate ACR-based HTTP Content Enrichment Rules

To associate an ACR with an HTTP content enrichment rule, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name> acce
ss-control-rule <access-control-rule-id>
   content-enrichment-rule <rule-name>
```

After performing the association of the ACR-based HTTP content enrichment rules, the node configuration resembles Example 7.

```
epg pgw rule-space rs-1
 access-control-rule 1
  content-enrichment-rule CE-01
```

Example 7 Associating HTTP Content Enrichment Rules

Associate PISC-based HTTP Content Enrichment Rules

To associate an HTTP-WSP rule with an HTTP content enrichment rule, include the following statement:

```
Ericsson(config)# epg pgw service-identification http-wsp-rule
<http-wsp-rule-name> term <term-id>
   then edit-content <http-edit-rule-name>
```

After performing the association of the PISC-based HTTP content enrichment rules, the node configuration resembles Example 8.

```
epg pgw service-identification http-wsp-rule http-r-1
 term 1
  name http-r
  then edit-content CE-01
```

Example 8 Associating HTTP Content Enrichment Rules

7.2 Associate IMAP Content Enrichment Rules

The IMAP content enrichment requires the operation `LOGIN` to be included in the service identification rule, because content enrichment only enriches this operation. If a packet is successfully matched to an IMAP rule and an IMAP rule term is associated with a content enrichment rule, the EPG applies all the content enrichment actions configured for the associated content enrichment rule. For more information, refer to PISC Configuration.

Associate PISC-based IMAP Content Enrichment Rules

To associate a content enrichment rule with an IMAP content enrichment rule, include the following statement:

```
Ericsson(config)# epg pgw service-identification imap-rule
<imap-rule-name> term <term-id> then
   edit-content <imap-edit-rule-name>
```

After performing the association of the PISC-based IMAP content enrichment rules, the node configuration resembles Example 9.

```
epg pgw service-identification imap-rule imap-r-1
 term 1
  name imap-r
  then edit-content CE-01
```

Example 9 Associating IMAP Content Enrichment Rules

7.3 Associate SMTP Content Enrichment Rules

The SMTP content enrichment requires the operation `MAIL` to be included in the service identification rule since this is the only operation enriched. If a packet is successfully matched to an SMTP rule and an SMTP rule term is associated with a content enrichment rule, the EPG applies all the content enrichment actions configured for the associated content enrichment rule. For more information, refer to PISC Configuration.

Associate PISC-based SMTP Content Enrichment Rules

To associate a content enrichment rule with an SMTP content enrichment rule, include the following statement:

```
Ericsson(config)# epg pgw service-identification smtp-rule
<smtp-rule-name> term <term-id> then
   edit-content <smtp-edit-rule-name>
```

After performing the association of the PISC-based SMTP content enrichment rules, the node configuration resembles Example 10.

```
epg pgw service-identification smtp-rule smtp-r-1
 term 1
  name smtp-r
  then edit-content CE-01
```

Example 10 Associating SMTP Content Enrichment Rules

7.4 Associate SSL/TLS Content Enrichment Rules

If a packet is successfully matched to an SSL/TLS rule and the SSL/TLS rule term is associated with a content enrichment rule, the EPG applies all the extension enrichment actions configured for the associated content enrichment rule.

Associate ACR-based SSL/TLS Content Enrichment Rules

To associate an ACR with an SSL/TLS content enrichment rule, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name> acce
ss-control-rule <access-control-rule-id>
   content-enrichment-rule <rule-name>
```

After performing the association of the ACR-based SSL/TLS content enrichment rules, the node configuration resembles Example 11.

```
epg pgw rule-space rs-1
 access-control-rule 1
  content-enrichment-rule CE-01
```

Example 11 Associating SSL/TLS Content Enrichment Rules

Associate PISC-based SSL/TLS Content Enrichment Rules

To associate a content enrichment rule with an SSL/TLS content enrichment rule, include the following statement:

```
Ericsson(config)# epg pgw service-identification ssl-tls-rule
<ssl-tls-rule-id> term <term-id> then
   edit-content <ssl-tls-edit-rule-name>
```

After performing the association of the PISC-based SSL/TLS content enrichment rules, the node configuration resembles Example 12.

```
epg pgw service-identification ssl-tls-rule ssltls-r-1
 term 1
  name ssltls-r
  then edit-content CE-01
```

Example 12 Associating SSL/TLS Content Enrichment Rules