|  |
| --- |
| 3GPP TR 33.737 V0.2.0 (2022-07) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on Authentication and Key Management for Applications (AKMA) phase 2;(Release 18) |
|   |
| *5G-logo_175px* | 3GPP-logo_web |
|  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 3

Introduction 4

1 Scope 5

2 References 5

3 Definitions of terms, symbols and abbreviations 5

3.1 Terms 5

3.2 Symbols 5

3.3 Abbreviations 5

4 Architectural assumptions 6

5 Key issues 6

5.1 Key Issue #1: Support for AKMA roaming scenario 6

5.1.1 Issue details 6

5.1.2 Security Threats 6

5.1.3 Potential security requirements 6

5.2 Key Issue #2: Introducing the Application proxy into AKMA 6

5.2.1 Key issue details 6

5.2.2 Security threats 7

5.2.3 Potential architectural and security requirements 7

6 Solutions 7

6.Y Solution #Y: <Solution Name> 7

6.Y.1 Introduction 7

6.Y.2 Solution details 7

6.Y.3 Evaluation 7

7 Conclusions 7

Annex A (informative): Change history 8

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# Introduction

Editor’s Note: This clause contains some background information for the study.

# 1 Scope

The present document studies key issues and potential solutions to support roaming aspects and the Authentication Proxy in AKMA, which is specified in TS 33.535[2]. Specifically, the present document:

- Investigates AKMA roaming architecture and requirements by taking regulatory compliance into account;

- Studies the architecture impact and procedures of introducing the Authentication Proxy (similar as the AP specified in GBA) into AKMA.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 33.535: " Authentication and key management for applications based on 3GPP credential in 5G （AKMA）".

[3] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) ".

[4] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[5] 3GPP TS 33.210: "Network Domain Security (NDS); IP network layer security ".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

<ABBREVIATION> <Expansion>

# 4 Architectural assumptions

The present document is based on the AKMA architecture and procedures specified in TS 33.535 [2]. The following figure shows the fundamental network model of AKMA, as well as the interfaces between them. Details of the AKMA requirements and procedures are documented in TS 33.535 [2].



Figure 4.1-1: Fundamental Network Model for AKMA

# 5 Key issues

Editor’s Note: This clause contains all the key issues identified during the study.

## 5.1 Key Issue #1: Support for AKMA roaming scenario

### 5.1.1 Issue details

AKMA roaming scenarios depend on UE and AF locations. There are different scenarios for AKMA roaming that need to be addressed:

Case 1: UE in VPLMN and accessing the AF (including both internal AF and external AF) in HPLMN.

Case 2: UE is in VPLMN and accessing the AF (including both internal AF and external AF) in VPLMN.

The AKMA roaming solutions should comply with LI requirements. It’s required either decrypted traffic or the means (e.g. providing keys) for law enforcement to decrypt the traffic should be provided to VPLMN. The LI requirements for access to keys are only for encryption, and in the AKMA case applies when the Ua\* protocol is encrypted.

### Editor’s Note: Further detailed LI requirements are FFS, according to the communication with SA3-LI.5.1.2 Security Threats

N/A

### 5.1.3 Potential security requirements

The AKMA architecture shall support the above mentioned AKMA roaming cases.

AKMA service shall be made to comply with the LI requirements.

## 5.2 Key Issue #2: Introducing the Authentication proxy into AKMA

### 5.2.1 Key issue details

TS 33.222 specifies the use of Authentication Proxy in GBA [2], where an Authentication Proxy (AP) is a proxy resides between the UE and ASs. It helps to reduce the consumption of authentication vectors and/or to minimize SQN synchronization failures, and relieves the AS of security tasks. Similarly, introducing such an authentication proxy in AKMA is beneficial where different application servers (or Application Functions in AKMA) reside in the same trust domain or in the same edge node. With the AP, these application servers can rely on the AP to execute AKMA procedures, which is more cost efficient than the case where each application servers execute AKMA procedures separately. AKMA is a potential solution in MEC, and it is possible that different application servers reside in the same edge cloud or belong to the same service vendor, it is beneficial to consider the feasibility of introducing a similar proxy in AKMA.

### 5.2.2 Security threats

Different Application servers reside in the same trust domain may execute AKMA procedures separately, leading to consumptions of AAnF generating AKMA keys and signalling resources.

### 5.2.3 Potential architectural and security requirements

The AKMA architecture may support an authentication proxy to perform the AF functionality residing between UE and AS(s), in order to save the consumption of signalling resources and AAnF computing resources.

The connection between AP and AS(s) should be secured.

# 6 Solutions

6.1 Solution #1: AKMA roaming solution for Ua\* encryption key

6.1.1 Introduction

AKMA roaming scenarios depend on UE and AF locations. Therefore, there are different scenarios for AKMA roaming that need to be addressed:

Case 1: UE in VPLMN#1 and accessing the AF located in HPLMN.

Case 2: UE is in VPLMN#1 and accessing the AF located in VPLMN#1.

The LI requirements for access to keys are only for the encryption, and in the AKMA case applies when the UA\* protocol is encrypted. The encryption keys could be derived from KAF (Example TLS profile defined in 33.535) or could be KAF itself. The encryption key could also be a completely different key, derived according to an application layer protocol, not defined by 3GPP. So LI should be compliant by AF in all the cases. However, the AF cannot do these without 3GPP assistance. If we break it down into the individual issues, then:

* How does AF know the LI requirements of VPLMN?
* How does AF provide the encryption keys to VPLMN where UE is attached?
* How does AF get the KAF from HPLMN?

Therefore, 3GPP should facilitate AF so that AF should be able to determine the UE roaming status and, accordingly, AF shall:

* provide the encryption key to VPLMN and/or
* stop the encryption and still provide the service to UE and may continue with only integrity protection and/or
* stop providing service to UE

6.1.2 Solution details



Figure 6.1.2.1: Roaming solution for Ua\* encryption key

Step 1-3 is the same as defined in TS 33.501[4] clause 6.1.3 and TS 33.535[2] Clause 6.1

4. The AUSF shall send the Naanf\_AKMA\_AnchorKey\_Register Request with SUPI, A-KID, KAKMA, and Registered SN ID to the home AAnF. The AKMA context is updated with this received Registered SN ID.

Note: AUSF will get the SN-name from the request of 'Nausf\_UEAuthentication\_Authenticate' from AMF.

5a. The UE requests an application session establishment request with A-KID towards the AF. The AF shall discover the AAnF and shall send the Naanf\_AKMA\_ApplicationKey\_Get request with A-KID and AF\_ID to the AAnF .

Note: If AF is not in the operator domain, then AF requests the AAnF via NEF. If AF is the HPLMN, then the AF request directly land at HPLMN AAnF.

5b. The home PLMN AAnF shall respond with Naanf\_AKMA\_ApplicationKey\_Get response containing Registered SN ID.

6. As the Registered SN ID is different from the PLMN in which the AF is located/connected, the AF shall decide:

- supporting pushing encryption keys to VPLMN#1, therefore AF shall discover the VPLMN#1 AAnF via Registered SN-ID and shall provide the encryption keys to VPLMN#1. VPLMN#1 AAnF shall store the encryption keys related to UE which may be used by LI if required (step 6a1 and step 6a2).

- shall not enable the encryption and may continue with the UE session with only integrity protection (step 6b).

- shall not provide the service to UE attached to other PLMN and shall reject the request (step 6c).

Editor's Note: The need to push encryption keys VPLMN AAnF is FFS.

Editor’s Note: Further solution details related to LI are FFS.

6.1.3 Solution Evaluation

TBD

## 6.2 Solution #2: New solution for AKMA roaming when both UE and AF are in VPLMN

### 6.2.1 Introduction

This solution addresses the requirement in KI#1 about the AKMA roaming.

This solution provides a method that when both UE and the AF in the same visited network. When the AF is inside 5GC, it can communicate with the UE’s AAnF in HPLMN directly. Otherwise, when AF is outside 5GC, it first connects to the NEF in HPLMN, and then the NEF will receive and send the message for the UE and the AAnF.

### 6.2.2 Solution details

Editor’s Note: The details of the AF being a regulatory control point for LI are FFS.

### 6.2.2.1 Architecture

 

Figure 6.2.2.1-1: Reference Model when UE and the AF are in the VPLMN

The Figure 6.2.2.1-1 shows an architecture model when UE and the AF are in the VPLMN.

### 6.2.2.2 Solution detail

#### 6.2.2.2.1 Deriving AKMA Application Key for a specific AF

Clause 6.2 in TS 33.535[2] applies with additionall descriptions:

- replace the AF with the AF in visited network.

- replace the UE with the UE in visited network.

Editor’s Note: The details of interconnect SBA security are FFS.

#### 6.2.2.2.2 AKMA Application Key request via NEF

As described in clause 6.3 in TS 33.535[2] applies with additionall descriptions:

- replace the NEF with the NEF in home network.

- replace the AF with the AF in visited network.

- replace the UE with the UE in visited network.

### 6.2.3 Evaluation

TBD

## 6.3 Solution #3: Roaming AKMA architecture of the AF in the HPLMN

### 6.3.1 Introduction

This solution addresses KI#1. This solution is proposed for the cases of regulatory control point deployment in which the VPLMN supports AKMA when AF located in the HPLMN.

### 6.3.2 Solution details

Figure 6.3.1-1 shows the SBA architecture that UE is roaming in a VPLMN and accesses the application deployed in the HPLMN. When UE is roaming in a VPLMN and accesses an application deployed in the HPLMN, the VPLMN does not need to detect whether the UE uses the AKMA service.



Figure 6.3.2-1: **The SBA architecture that UE is roaming in a VPLMN and accesses the application deployed in the HPLMN**

Figure 6.3.1-2 shows the architecture that UE is roaming in a VPLMN and accesses the application deployed in the HPLMN. The UE accesses the home network deployment application. Like the third party deployment service, the VPLMN can only detect the data flow through UPF in the VPLMN (if the data between the UE and application do not encrypt). In this case, the regulatory control point should be UPF in the VPLMN.



Figure 6.3.2-2: **The architecture that UE is roaming in a VPLMN and accesses the application deployed in the HPLMN (\*regulatory control point)**

Editor’s Note: The details of the UPF being a regulatory control point for LI are FFS.

Editor’s Note: How LI requirements are to be fulfilled is FFS.

### 6.3.3 Solution Evaluation

TBD

## 6.4 Solution #4: Roaming AKMA architecture of the AF in the VPLMN

### 6.4.1 Introduction

This solution addresses KI#1. This solution is proposed for the cases of regulatory control point deployment in which the VPLMN supports AKMA when AF located in the VPLMN.

### 6.4.2 Solution details

Figure 6.4.1-1 shows the SBA architecture that UE is roaming in a VPLMN and accesses the application deployed in the VPLMN. The home network (HPLMN) needs an agreement with the service network (VPLMN) to use the AKMA service deployed in the home network. In this scenario, the service network can sense the AKMA service used by the UE. For this scenario, AF is located inside the VPLMN and needs to find the AAnF of the home network through the NEF of the home network.



Figure 6.4.2-1: **The SBA architecture that UE is roaming in a VPLMN and accesses the application deployed in the VPLMN**

Figure 6.4.1-2 shows the architecture that UE is roaming in a VPLMN and accesses the application deployed in the VPLMN. As described in clause 6.3 of the 3GPP TS 33.535[2], the AF needs to obtain the KAF from the AAnF through the NEF. Therefore, the regulatory control point in Figure 6.4.1-2 can be AF in the VPLMN.



Figure 6.4.2-2: **The architecture that UE is roaming in a VPLMN and accesses the application deployed in the VPLMN (\*regulatory control point)**

Editor’s Note: The details of the AF being a regulatory control point for LI are FFS.

Editor’s Note: How LI requirements are to be fulfilled is FFS.

### 6.4.3 Solution Evaluation

TBD

## 6.5 Solution #5: AKMA anchor key registration to the AAnF in VPLMN after primary authentication

### 6.5.1 Introduction

This solution addresses the KI #1. The proposed solution registers AKMA anchor key (KAKMA) and A-KID to the AAnF in VPLMN after primary authentication for UE in the same manner of KAKMA and A-KID registration to the AAnF in HPLMN. Once the KAKMA and the A-KID are registred in AAnFs in VPLMN and HPLMN, the UE in VPLMN is able to access to both VPLMN AF and HPLMN AF. Moreover, even if KAUSF which is a root key of the KAKMA is changed by new primary authetnciaon, there is no need additional key update procedure for the VPLMN AAnF since the new KAKMA and A-KID will replace the old keys whenever primary authentication is performed.

### 6.5.2 Solution details



Figure 6.5.2-1: AKMA anchor key registration to the AAnF in VPLMN after primary authentication

1. The AUSF requests authentication information to the UDM to acquire subscription information and authentication method in primary authentication procedure.

2. The UDM responses with the Authentication Vector. The AKMA indication and the RID may be included in the response if the UE needs AKMA anchor key generation.

3. If the AUSF receives the AKAM indication from the UDM, the AUSF shall store KAUSF and generate AKMA Anchor Key (KAKMA) and the A-KID. The UE shall generate the KAKMA and the A-KID if the primary authentication procedure is completed.

4. If the keys generation is completed, the AUSF shall request to the HPLMN AAnF to register A-KID and KAKMA. The selection of the AAnF is described in TS 33.535 clause 6.7 [2].

5. The AAnF in HPLMN responses to the AUSF after key registration completed.

6. If the AUSF recognizes the UE is for roaming from SN-name previously received in the primary authentication, the AUSF selects the AAnF in VPLMN to register KAKMA and A-KID based on Visited Network Information by querying the NRFs between VPLMN and HPLMN.

NOTE: For the service discovery from HPLMN to VPLMN to select the AAnF in VPLMN, new procedures for service discovery procedure would be required.

7. The AAnF in VPLMN responses to the AUSF after key registration completed.

NOTE: For the service discovery from HPLMN to VPLMN to select the AAnF in VPLMN, new procedures for service discovery may be needed.

Editor’s Note: Further solution details related to LI are FFS.

Editor’s Note: The details of vAANF selection by the AUSF is FFS.

Editor’s Note: Whether The AUSF always pushes the AKMA contxt depends on LI regulatory requirement and is FFS.

### 6.5.3 Evaluation

TBD

## 6.6 Solution #6: AKMA roaming with VAAnF for LI

### 6.6.1 Introduction

This solution is addressing Key Issue #1: Support for AKMA roaming scenario, especially the scanrio when the UE is in VPLMN and trying to access the HPLMN AF.

The issue of LI for AKMA roaming was described as follows: if the UE is roaming in a VPLMN, then the UE builds up a secure tunnel to an AF in the HPLMN and since the credentials used for the encryption are based on the 3GPP derived keys, the VPLMN must be able to perform LI. This is not possible compared to GBA, where the NAF and tunnel endpoint is located in the VPLMN.

Further it cannot be implied that the AF is always in the VPLMN for roaming scenarios, for typical deployments it can be a 3rd party AF in a data network.

If the VPLMN needs to perform LI, then the VPLMN needs to be enhanced to store the SUPI and the encryption key e.g. with a local AAnF. It is recommended to further also only provide the KAF to the VPLMN for the service the UE is currently requesting from the AF. In case the VPLMN is not enhanced but has a strong LI requirement for AKMA, the AF should not get the KAF and should get an indication that NULL encryption has to be used.

### 6.6.2 Solution details

The solution proposes to introduce a VAAnF in the VPLMN in order to store the connection details of the UE roaming in that VPLMN to the AF outside that VPLMN. The differences to the normal procedures of TS 33.535 are described below.



Figure 6.6.2-1: Deriving KAKMA after primary authentication

Additionally to the other AKMA related parameters, the AUSF provides also the SN name to the AAnF in the HPLMN in step 4. The SN name is later used to determine whether the Ue is roaming and to select an appropriate AAnF in the VPLMN (VAAnF) for storing the AKMA connection details.



Figure 6.6.2-2: KAF generation from KAKMA and provisioning to VPLMN

In step 3, the HAAnF derives the AKMA Application Key (KAF) from KAKMA if it does not already have KAF.

In step 4, the HAAnF detects based on the SN name that the UE is roaming and if the VPLMN has AKMA LI enhancements, then the HAAnF provides the KAF and the KAF expiration time together with the SUPI of the UE to the VAAnF in the VPLMN for storing the AKMA LI context. The VPLMN AKMA capabilities and policies may be configured in the HAAnF and may be based on SLAs.

Editor’s Note: How to address the case that a VPLMN operator does not support AKMA and is required to perform LI is FFS

Editor’s Note: Further solution details related to LI are FFS.

### 6.6.3 Evaluation

TBD

## 6.7 Solution #7: Introducing AP into AKMA

### 6.7.1 Introduction

TS 33.222 specifies the use of Authentication Proxy in GBA [3], where an Authentication Proxy (AP) is a proxy resides between the UE and ASs. It helps to reduce the consumption of authentication vectors and/or to minimize SQN synchronization failures, and relieves the AS of security tasks. Similarly, introducing such an authentication proxy in AKMA is beneficial where different application servers reside in the same trust domain or in the same edge node. With the AP, these application servers can rely on the AP to execute AKMA procedures, which is more cost efficient than the case where each application servers execute AKMA procedures separately. AKMA is a potential solution in MEC, and it is possible that different application servers reside in the same edge cloud or belong to the same service vendor, it is beneficial to consider the feasibility of introducing a similar proxy in AKMA.

### 6.7.2 Solution details

### 6.7.2.1 Architecture of using AP

An Authentication Proxy (AP) is a proxy which takes the role of an AF and delegates a group of ASs. It may reside between the UE and the AS as depicted in the figures below. The AP helps the ASs behind the AP to execute AKMA procedures to save the consumption of signalling resources and AAnF computing resources. It may also relieve the AS of security tasks. The use of an AP is fully compatible with the architecture specified in TS 33.535 [2].

The AP can assure the ASs that the request is coming from an authorized subscriber of the MNO.



Figure 6.7.2.1-1: Use of AP when AP is internal



Figure 6.7.2.2-1: Use of AP when AP is external

Editor’s Note: Configuration of AP’s FQDN is FFS.

### 6.7.2.2 AP-AS reference point

The HTTP protocol is run over the AP-AS reference point. Confidentiality and integrity protection can be provided for the reference point between the AP and the AS using NDS/IP mechanisms as specified in TS 33.210 [5]. For traffic between different security domains, the Za reference point shall be operated. For traffic inside a security domain, it is up to the operator to decide whether to deploy the Zb reference point.

### 6.7.2.3 Example of using AP for TLS tunnels

When the TLS based protocol is used as Ua\* profile, the AP can be used to handle the TLS security relation with the UE and relieves the application server (AS) of this task. When an HTTPS request is destined towards an application server (AS) behind an AP, the AP terminates the TLS tunnel and performs UE authentication. The AP proxies the HTTP requests received from UE to one or many application servers. The AP may add an assertion of identity of the subscriber for use by the AS, when the AP forwards the request from the UE to the AS.



Figure 6.7.2.3-1: Use of AP for TLS tunnels when AP is external



Figure 6.7.2.3-2: Use of AP for TLS tunnels when AP is external

### 6.7.3 Evaluation

Editor’s Note: FFS

# 7 Conclusions

Editor’s Note: This clause contains the agreed conclusions that will form the basis for any normative work.

Annex A (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-05 | SA3#107-e |  |  |  |  | TR Skeleton | 0.0.0 |
| 2022-05 | SA3#107-e | S3-221169 |  |  |  | S3-221288, S3-220812, S3-221289, S3-221218 | 0.1.0 |
| 2022-07 | SA3#107Adhoc-e | S3-221687 |  |  |  | S3-221634, S3-221635, S3-221662, S3-221651, S3-221652, S3-221596, S3-221592, S3-221688 | 0.2.0 |