**ATIS-1x000xx**

ATIS Standard on

**SHAKEN Roadmap**

**Alliance for Telecommunications Industry Solutions**

Approved Month DD, YYYY

**Abstract**

This Technical Report provides a roadmap view of the subtending suite of ATIS standards, technical reports, and requirements documents showing the applicability of particular standard specifications in the context of enabling deployment of the needed National Security/Emergency Preparedness (NS/EP) priority related functions and capabilities supporting end-to-end priority communications in Next Generation Networks (NGNs). The ATIS set of standards includes national specific applications of 3GPP, IETF and ITU-T specifications for the support of ETS. This document includes a roadmap of the dependent 3GPP, IETF and ITU-T specifications and standards.

**Foreword**

**Revision History**

| **Date** | **Version** | **Description** | **Author** |
| --- | --- | --- | --- |
|  |  |  |  |

**Table of Contents**

[INSERT]

**Table of Figures**

[INSERT]

**Table of Tables**

[INSERT]

# Scope, Purpose, & Application

## Scope

There are numerous industry standards, technical reports, and requirements documents addressing various aspects for

This Technical Report (TR) provides a roadmap view of the subtending suite of IPNNI standards, technical reports, and requirements documents showing the applicability of particular standard specifications in the context of enabling deployment of Signature-Based Handling of Asserted Information Using Tokens (SHAKEN). This TR includes a roadmap of the dependent 3GPP, IPNNI and IETF specifications and standards.

## Purpose

The purpose of this TR is to provide a consolidated view of various SHAKEN related specifications and provide a roadmap view to enable SHAKEN deployment in NGNs. The objective is to provide a roadmap view showing the applicability of particular specifications to specific network layer, network procedure, interfaces or network element functional capabilities and segments making up the end-to-end NGN infrastructure.

## Application

This document is applicable to the support of SHAKEN in the public NGN infrastructure.

# Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

**ATIS**

[ATIS-1000074] *Signature-based Handling of Asserted Information using Tokens (SHAKEN)*

[ATIS-0300251.2007 (R2012)] *Codes for Identification of Service Providers for Information Exchange*

[ATIS-1000080] *Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management*

[ATIS-1x000xx] *Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators*

**3GPP**

[TR xx.yyy]

**IETF**

RFC 2986, *PKCS #10: Certification Request Syntax Specification Version 1.7*

RFC 3325, *Private Extensions to SIP for Asserted Identity within Trusted Networks.*1

RFC 3261, *SIP: Session Initiation Protocol.*1

RFC 3326, *The Reason Header Field for the Session Initiation Protocol (SIP).*1

RFC 3647, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*

RFC 3966, *The tel URI for Telephone Numbers*

RFC 4949, *Internet Security Glossary, Version 2*

RFC 5217, *Memorandum for Multi-Domain Public Key Infrastructure Interoperability*

RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*1

RFC 5905, *Network Time Protocol Version 4 (NTPv4)*

RFC 7159, *The JavaScript Object Notation (JSON)*

RFC 7231, *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content”*

RFC 7375, *Secure Telephone Identity Threat Model*

RFC 7515, *JSON Web Signatures (JWS)*

RFC 7516, *JSON Web Algorithms (JWA)*

RFC 7517, *JSON Web Key (JWK)*

RFC 7519, *JSON Web Token (JWT)*

RFC 8225 , *Persona Assertion Token.*[[1]](#footnote-1)

RFC 8224, *Authenticated Identity Management in the Session Initiation Protocol.*1

RFC 8226, *Secure Telephone Identity Credentials: Certificates.*1

draft-ietf-stir-passport-shaken-02, PASSporT SHAKEN Extension (SHAKEN)

draft-ietf-acme-acme, *Automatic Certificate Management Environment (ACME).*

draft-ietf-acme-service-provider, *ACME Identifiers and Challenges for VoIP Service Providers.*

# Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < <http://www.atis.org/glossary> >.

## Definitions

None.

## Acronyms & Abbreviations

|  |  |  |
| --- | --- | --- |
| 3GPP | 3rd Generation Partnership Project | |
| ACME | Automated Certificate Management Environment (Protocol) | |
| CA | Certification Authority | |
| CP | Certificate Policy | |
| CPS | Certification Practice Statement | |
| CSR | Certificate Signing Request | |
| DN | Distinguished Name | |
| DNS | Domain Name System | |
| HTTPS | Hypertext Transfer Protocol Secure | |
| IETF | [Internet Engineering Task Force](http://www.ietf.org/rfc.html) | |
| JSON | JavaScript Object Notation | |
| JWA | JSON Web Algorithms | |
| JWK | JSON Web Key | |
| JWS | JSON Web Signature | |
| JWT | JSON Web Token | |
| NECA | National Exchange Carrier Association | |
| NNI | Network-to-Network Interface | |
| NRRA | National/Regional Regulatory Authority | |
| OCN | Operating Company Number | |
| OCSP | Online Certificate Status Protocol | |
| PASSporT | Personal Assertion Token | |
| PKI | Public Key Infrastructure | |
| PKIX | Public Key Infrastructure for X.509 Certificates | |
| PSTN | Public Switched Telephone Network | |
| SHAKEN | Signature-based Handling of Asserted information using toKENs | |
| SIP  REST | Session Initiation Protocol  Representational state transfer (REST) | |
| SKS | Secure Key Store | |
| SMI | Structure of Management Information | |
| SP | Service Provider | |
| SP-KMS | SP Key Management Server | |
| STI | Secure Telephone Identity | |
| STI-AS | Secure Telephone Identity Authentication Service | |
| STI-CA | Secure Telephone Identity Certification Authority | |
| STI-CR | Secure Telephone Identity Certificate Repository | |
| STI-GA | Secure Telephone Identity Governance Authority | |
| STI-PA | Secure Telephone Identity Policy Administrator | |
| STI-VS | Secure Telephone Identity Verification Service | |
| STIR | Secure Telephone Identity Revisited | |
| TLS | Transport Layer Security | |
| TN | Telephone Number | |
| URI | Uniform Resource Identifier | |
| VoIP | Voice over Internet Protocol | |

# Roadmap Overview

This section describes the methodology used to categorize and provide a roadmap view of the applicable documents.

## Reference Model

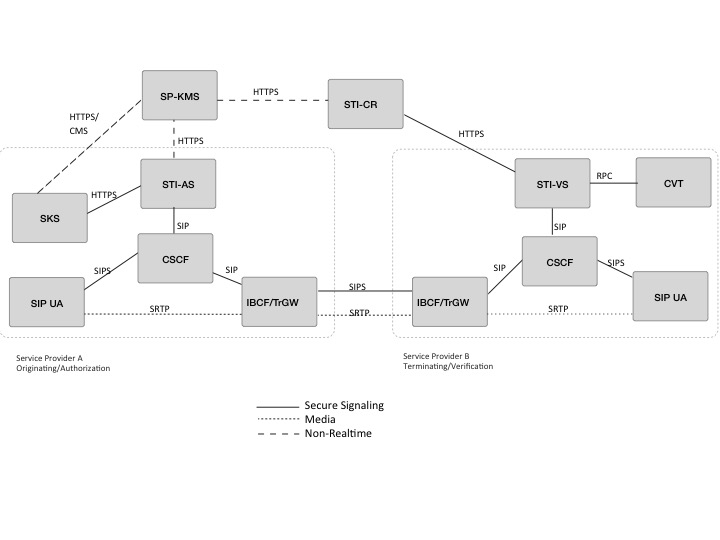


Figure 4.1 –Reference Model

# ATIS/SIP Forum IP Network-Network Interface (IPNNI) Task Group

The ATIS/SIP Forum IPNNI Task group has developed specifications defining an ecosystem to support the SHAKEN framework in VoIP networks as follows:

* [ATIS-1000074] *Signature-based Handling of Asserted Information using Tokens (SHAKEN)*
* [ATIS-1000080] *Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management*
* [ATIS-1x000xx] *Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators*
* [ATIS-1x000xx] Framework for Display of Verified Caller ID
* [ATIS-1x000xx] TN-PoP [Editor’s note: should we include this?]

An overview of each of the specifications, along with IETF dependencies are provided in the following sections. Section 7 of this document provides a summary of the IETF specifications, along with the key dependencies on other IETF specifications.

## SHAKEN Framework (ATIS-1000074) and related documents

The Signature-Based Handling of Asserted Information using toKENs (SHAKEN) framework provides a model for deployment of Secure Telephone Identity (STI) technologies to provide end-to-end cryptographic authentication and verification of the telephone identity for calling parties in Voice over IP service provider networks. Additional information about the call origination is also captured at call origination and transported to the terminating network. The SHAKEN framework is based on the use of Session Initiation Protocol (SIP) extensions to sign and validate the calling party identity.

### IETF dependencies

* RFC 3261: SIP: Session Initiation Protocol
* RFC 3325: Private Extensions to SIP for Asserted Identity within Trusted Networks.
* RFC 3326: The Reason Header Field for the Session Initiation Protocol (SIP)
* RFC 3966: The tel URI for Telephone Numbers
* RFC 8224: Authenticated Identity Management in the Session Initiation Protocol*.*
* RFC 8225: Persona Assertion Token
* RFC 8226: Secure Telephone Identity Credentials: Certificates
* draft-ietf-stir-passport-shaken SHAKEN PASSporT extensions

### Related SHAKEN Framework and Informational documents

* RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

The following proposal, referred to as “AT&T’s Tagging Optimization”, is premised on the fact that many calls originating in a service provider’s network stay within that network:

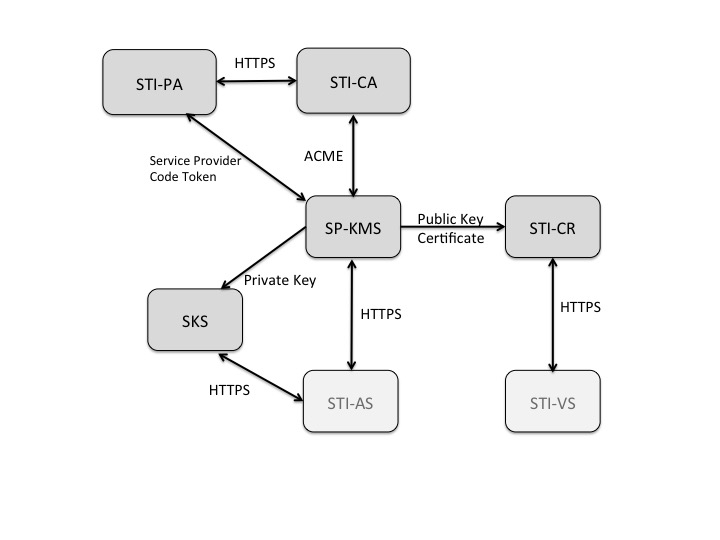
<https://access.atis.org/apps/group_public/download.php/33957/IPNNI-2017-00037R000.pdf>

So, rather than signing the calls at origination, the information that would be required to build the PASSporT is captured at the time of call in origination in SIP P- headers. If, and when, the call leaves the service provider’s network, the P- headers are used to populate the fields in the PASSporT by invoking the SSVS API.

## SHAKEN: Governance and Certificate Management (ATIS-1000080)

This specification expands the SHAKEN framework to introduce a governance model and X.509 Public Key Infrastructure (PKI) certificate management procedures. The certificate management procedures provide mechanisms for creating and validating certificates as well as a means for verification of the associated digital signature to allow identification of illegitimate use of the

The following diagram identifies the functional elements and interfaces involved in the Certificate Management Procedures:



### IETF dependencies

* RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
* RFC 7231Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content
* RFC 7519JSON Web Token (JWT*)*
* RFC 8226 Secure Telephone Identity Credentials: Certificates
* draft-ietf-acme-service-provider SHAKEN extensions to support use of Service Provider Code

### Certificate Management informational documents

* RFC 4949 Internet Security Glossary, Version 2
* RFC 5217 Memorandum for Multi-Domain Public Key Infrastructure Interoperability
* RFC 5905Network Time Protocol Version 4 (NTPv4)
* RFC 7375 Secure Telephone Identity Threat Model.

The following presentations provide overviews related to the SHAKEN Certificate Management Framework:

* Overview of SHAKEN Certificate Management framework as defined in ATIS-1000080:

[https://access.atis.org/apps/group\_public/download.php/35614/IPNNI-2017-00085R001.pdf](https://access.atis.org/apps/group_public/download.php/35614/IPNNI-)

* ACME Protocol Overview:

<https://access.atis.org/apps/group_public/download.php/35615/IPNNI-2017-00084R001.pdf>

* Overview of SHAKEN's use of ACME:

[https://access.atis.org/apps/group\_public/download.php/35605/IPNNI-2017-00091R000.pdf](https://access.atis.org/ap)

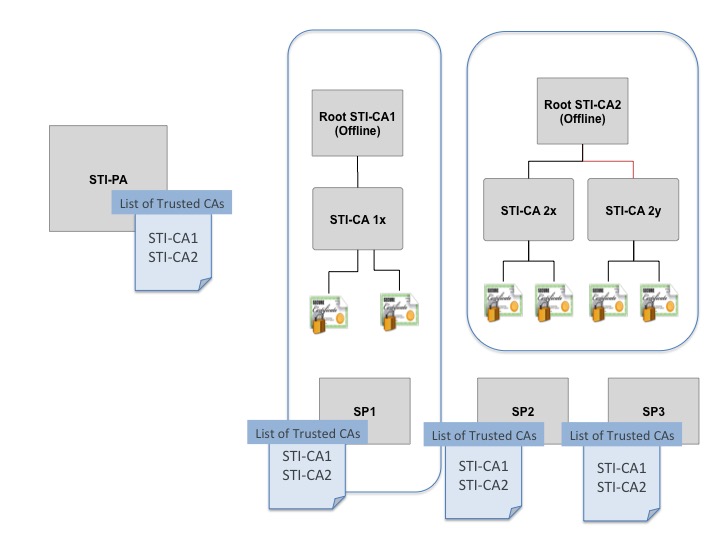
## Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrator (ATIS-1x000xx)

This document introduces operational and management considerations for STI Certification Authorities (STI-CAs) within the context of the SHAKEN framework [ATIS-1000074] and the SHAKEN: Governance Model and Certificate Management framework [ATIS-1000080]. This document focuses on the operational and management aspects that impact the authentication and verification services, as well as general Certification Authority (CA) practices and policies. The document addresses the STI-PA operational aspects of managing the list of STI-CAs and authorization of Service Providers to obtain STI certificates.

The following diagram highlights the functional elements and interfaces described in this document:



The following diagram illustrates the Trust Model for the SHAKEN Certificate Management framework, underlying the functionality that is provided by the STI-PA:



### IETF dependencies

* RFC 3647Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
* RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
* RFC 7231Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content
* RFC 7519JSON Web Token (JWT*)*
* RFC 8224 Authenticated Identity Management in the Session Initiation Protocol (SIP)
* RFC 8226 Secure Telephone Identity Credentials: Certificates

### Operational and Management Considerations for SHAKEN STI-CAs and STI-PAs informational documents

* RFC 4949 *Internet Security Glossary, Version 2*
* RFC 5217 Memorandum for Multi-Domain Public Key Infrastructure Interoperability
* RFC 5905 *Network Time Protocol Version 4 (NTPv4)*

The following document provides an overview of the Operational and Management Considerations for SHAKEN STI-CAs and STI-Pas document:

<http://access.atis.org/apps/group_public/document.php?document_id=35562&wg_abbrev=ipnni>

## Authentication/Verification Service API

This document introduces an optional API between the Authentication and Verification Services and a centralized signing and signature validation server to the SHAKEN Framework [ATIS-1000074]. In many cases the signing and validation of the signature require cryptographic processors such as Hardware Security Modules (HSMs) for optimal performance. This API facilitates a model whereby the core AS functionality is deployed on an existing application server in the service provider’s network as opposed to a standalone AS server.

The following diagram highlights the functional model introduced to support the API:

[Editor’s note: Insert diagram.]

## Display Framework:

This document provides guidelines related to the display of verified Caller ID information on the User Equipment (UE) in a uniform manner. The guidelines are in the form of best practices based on a review of industry standards and studies on the effectiveness of warning signs and human factors related to the reading and comprehension of variable messages (text and symbolic). The guidelines are not prescriptive, but rather are recommendations for consideration by all stakeholders (service providers, equipment manufacturers and analytics providers) in the deployment of verified Caller ID displays and composition of its related messages.

[Editor’s note: insert diagram]

## SHAKEN for Enterprise/PBX - Proof of Number Possession

This document defines an extension to the base SHAKEN framework that enables an STI service provider to delegate authority, in the form of a “proof-of-possession”, for a subset of its telephone numbers to a non-STI entity. The non-STI entity can then use this “proof-of-possession” to provide cryptographic proof to STI verification services that it has authority to attest that the customer can legitimately originate calls from the delegated TNs. The document defines the certificate management procedures as well as the authentication and verification procedures specific to the TN Proof-of-Possession (TN PoP).

# 3GPP

[Editor’s note: See IPNNI-2018-000045R001]

# IETF

This section provides a roadmap of dependent IETF RFCs. The SHAKEN framework [ATIS-1000074] is dependent upon IETF Session Initiation Protocol (SIP) RFCs as well as the RFCs developed in the Secure Telephone Identity Revisited (STIR) WG. The SHAKEN Certificate Management framework is dependent upon core Public Key Infrastructure (PKI) specifications as well as those in the Automated Certificate Management (ACME) WG specifications. Note that this is not a complete list of RFCs required as each of the RFCs identified below also has dependencies – a complete list of these can be found for each document in the IETF datatracker.

The IETF RFCs are organized into two tables as follows:

* Documents providing normative requirements and/or protocols for support of SHAKEN Framework and SHAKEN Governance and Certificate Management Framework

|  |  |  |  |
| --- | --- | --- | --- |
| Document | Title | Description | Key Dependencies |
| RFC3325 | *Private Extensions to SIP for Asserted Identity within Trusted Networks.* | Defines the P-Asserted-Identity header field that allows a Service Provider to assert an Identity other than what’s in the To Header field. In the context of SHAKEN, the P-Asserted-Identity header field, if present, is used to populate the PASSporT “orig” field . | RFC 3261 |
| RFC 3261 | *SIP: Session Initiation Protocol.* | Core SIP Protocol specification |  |
| RFC 3326 | *The Reason Header Field for the Session Initiation Protocol (SIP).* |  | RFC 3261 |
| RFC 3966 | *The tel URI for Telephone Numbers* | The STIR/SHAKEN is premised on the use of tel URIs in the TO, FROM and PAI header fields in the SIP signaling. | RFC 3261 |
| RFC 5280 | *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*1 | Defines the including the format for the PKI certificate extended by STIR per |  |
| RFC 7159 | *The JavaScript Object Notation (JSON)* | The format for the contents of the PASSporT is based on JSON. | Obsoleted by RFC 8259 |
| RFC 7231 | *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content”* | The interfaces between the Service Provider and the STI-PA and STI-CA are based on HTTP. |  |
| RFC 7515 | *JSON Web Signatures (JWS)* | JSON Web Signature (JWS) represents content secured with digital signatures using JSON-based data structures. | RFC 7159, RFC 7518 |
| RFC 7516 | *JSON Web Encryption (JWE)* | JSON Web Encryption (JWE) represents encrypted content using JSON-based data structures. | RFC 7159, RFC 5280, RFC 7518 |
| RFC 7517 | *JSON Web Key (JWK)* | A JSON Web Key (JWK) is a JavaScript Object Notation (JSON) data structure that represents a cryptographic key. This specification also defines a JWK Set JSON data structure that represents a set of JWKs. | RFC 7159, RFC 7518 |
| RFC 7518 | *JSON Web Algorithm* | This specification registers cryptographic algorithms and identifiers to be used with the JSON Web Signature (JWS), JSON Web Encryption (JWE), and JSON Web Key (JWK) specifications. | RFC 7159 |
| RFC 7519 | *JSON Web Token (JWT)* | The PASSporT included in the SIP Identity header field is encoded as a JWT. | RFC 7159, RFC 7515, RFC 7516, RFC 7517, RFC 7518 |
|  |  |  |  |
| RFC 8224 | *Authenticated Identity Management in the Session Initiation Protocol.*1 | Defines the syntax and semantics for the SIP Identity header field, updating RFC 4447. | RFC 8226 |
| RFC 8225 | *Persona Assertion Token.*[[2]](#footnote-2) | Defines the syntax and semantics for the PASSporT field in the SIP Identity header field. | RFC 8224, RFC 7519 |
| RFC 8226 | *Secure Telephone Identity Credentials: Certificates.*1 | Defines the procedures for the use of PKI in the context of STIR. Defines an extension to the RFC 5280 Certificate format to include TNs and Service Provider codes. | RFC 5280 |
| RFC 8259  (Obsoletes RFC 7519) | *The JavaScript Object Notation (JSON)* | The format for the contents of the PASSporT is based on JSON. |  |
| draft-ietf-stir-passport-shaken | PASSporT SHAKEN Extension (SHAKEN) | Defines the syntax and semantics for the SHAKEN specific extensions to the PASSporT. | RFC 8225, ATIS-1000074 |
| draft-ietf-acme-acme | *Automatic Certificate Management Environment (ACME).* | Defines the protocol used by the Service Provider to request certificates from the STI-CA. | RFC 2986 |
| draft-ietf-acme-service-provider, | *ACME Identifiers and Challenges for VoIP Service Providers.* | Defines the SHAKEN specific mechanism for the ACME challenge response based on the Service Provider Code Token. | draft-ietf-acme-acme, ATIS-1000080 |

* Documents providing general reference material and informational guidelines, related to the normative SHAKEN specifications.

|  |  |  |
| --- | --- | --- |
| Document | Title | Description |
| RFC 3647 | *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* | Provides a framework and details for Certificate Policies (CPs) to be established by the STI-PA and Certification Practice Statements (CPSs) to be provided by STI-CAs during the approval process. |
| RFC 4949 | *Internet Security Glossary, Version 2* | Defines terminology used for PKI, certificates, etc. that provide the baseline for terminology used in ATIS-1000074, ATIS-1000080 and IPNNI-2018-00004Rxxx |
| RFC 5217 | *Memorandum for Multi-Domain Public Key Infrastructure Interoperability* | Defines a model for Multi-domain PKI that defines considerations for the SHAKEN Trust Domain model introduced in ATIS-1000080 and IPNNI-2018-00004Rxxx |
| RFC 5905 | *Network Time Protocol Version 4 (NTPv4)* | Recommended to be implemented by the STI-PA, STI-CA and Service Providers to ensuring time is aligned to ensure consistency and predictability with regards to the expiry of certificates, Service Provider Code tokens along with various timestamps (e.g., IAT in the PASSporT). |
| RFC 7375 | *Secure Telephone Identity Threat Model* | Introduces the threat model for STIR, which imposes some requirements on the signaling solution and certificate management procedures. |

1. Available from the Internet Engineering Task Force (IETF) at: < <https://www.ietf.org/> >. [↑](#footnote-ref-1)
2. Available from the Internet Engineering Task Force (IETF) at: < <https://www.ietf.org/> >. [↑](#footnote-ref-2)