COMMUNICATIONS
ALLIANCE LTD

INDUSTRY GUIDELINE

G608:2004

EIE INFRASTRUCTURE COMMON NETWORK SPECIFICATION

G608:2004 EIE Infrastructure Common Network Specification Industry Guideline

First published as ACIF G608:2002
Second edition as ACIF G608:2004

G608:2004 was re-published in 2015 as a Communications Alliance document to reflect the organisational name change from ACIF to Communications Alliance. No other change to content has been made.

Communications Alliance Ltd was formed in 1997 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services.

Disclaimers

1) Notwithstanding anything contained in this Industry Guideline:

   a) Communications Alliance disclaims responsibility (including where Communications Alliance or any of its officers, employees, agents or contractors has been negligent) for any direct or indirect loss, damage, claim, or liability any person may incur as a result of any:

      i) reliance on or compliance with this Industry Guideline;

      ii) inaccuracy or inappropriateness of this Industry Guideline; or

      iii) inconsistency of this Industry Guideline with any law; and

   b) Communications Alliance disclaims responsibility (including where Communications Alliance or any of its officers, employees, agents or contractors has been negligent) for ensuring compliance by any person with this Industry Guideline.

2) The above disclaimers will not apply to the extent they are inconsistent with any relevant legislation.

Copyright

EXPLANATORY STATEMENT

This Explanatory Statement is to be read in conjunction with the G608:2004 EIE Infrastructure Common Network Specification Industry Guideline, "the Guideline".

This Explanatory Statement outlines the background, scope, objectives, processes and procedures described in the Code. The anticipated costs and benefits are also discussed.

The Guideline replaces ACIF G608:2002 EIE Infrastructure Common Network Specification Industry Guideline.

Expressions used in this Explanatory Statement have the same meaning as in the Guideline.

Background

The need for an Electronic Information Exchange Common Network (EIEnet) evolved from a long process of reviewing the way that industry does business.

The Australian Communications Industry Forum (ACIF), the Service Provider's Industry Association (SPAN) and Telstra (AST) Working Groups were established in March 1998 to find solutions to identified problems in commercial churn, inter-operator billing and wholesale service provisioning & restorations, produced recommendations that led to the forming of the Telecommunications On-Line Initiative (TOLI).

TOLI identified a number of activities required to progress the on-line initiative in the short to medium term.

The TOLI identified objectives that include, but were not limited to:

- the telecommunications industry should be characterised by on-line electronic processes as opposed to paper based processes;
- wherever possible and appropriate for the particular transaction, electronic processes should allow more than the electronic transmission of data; and
- establishing on-line processes should be to facilitate competition and remove artificial barriers to entry. Accordingly, requirements for on-line interfacing should not themselves become barriers to entry.

This subsequently resulted in the establishment of the EIE Reference Panel under the direction of the ACIF and the formation of Working Committees to progress components of the initiative, titled the Electronic Information Exchange Programme.

The EIE Programme seeks to address the industry needs for on-line electronic capability for the exchange of information between telecommunications operators and to achieve the above objectives.

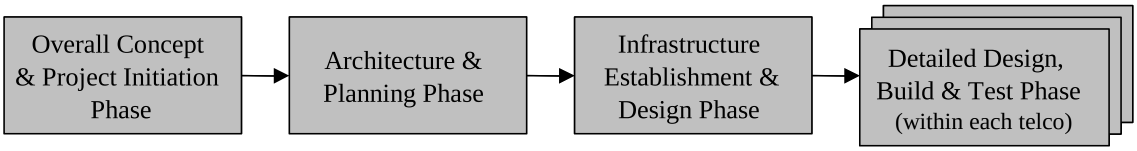
The industry recognised that the programme needed to be phased in with activities for planning and building infrastructure and capability, while fostering an industry mind-set favourably disposed towards standard interchange arrangements. Key to this approach is actual usage through pilot projects, incentives for early adoption and ongoing application development.

The Architecture and Planning Phase produced various documents which specified the requirements for the Administration Node and Business Process Models and Transactions. These include:

- Infrastructure Inventory of Systems
- Architecture Requirements
- Security Addendum to the Architecture Requirements
- Infrastructure Architecture
- Business Process Hierarchy Attributes
- Business Process Inventory
- Business Process Models
- Process Requirements
- Data Repository Glossary
- EIE Message Derivation Process
- Repository Framework and Requirements
- EIE Operations Manual
- Resale Operations Manual
- Transaction to EIE Data Attribute Matrix
- EIE Change Management
- EIE Project Methodology
- Final Report V4

The Infrastructure Establishment and Design Phase covers the design and establishment of the Administration Node, the EIEnet and the messaging solution. The Administration Node has been developed and delivered.

The Detailed Design, Build and Test Phase covers the implementation of the EIE in each operator organisation.


Overall Concept & Project Initiation Phase
Architecture & Planning Phase
Infrastructure Establishment & Design Phase
Detailed Design, Build & Test Phase (within each telco)

The EIEnet is intended to enhance inter-operator arrangements by providing interconnectivity for the transfer of electronic transactions between Participants

The EIE Infrastructure Requirements

The EIE Infrastructure requirements are derived from the Terms of Reference of the EIE Reference Panel:

"To develop effective and efficient Business-to-Business (B2B) e-commerce systems to streamline industry interworking. This includes setting standards for on-line processes and the architecture through which on-line processes can take place."

The requirements that are most demanding of any infrastructure are non-functional. This is especially the case with EIE Infrastructure since the solution is required to support known and unforeseen inter-operator processes. The EIE Infrastructure non-functional requirements include:

- Openness – open to multiple operators and their business and technical systems

- Extensibility – able to expand in capability as required

- Affordability – the cost of implementation should not restrict participation

- Scalable – EIE must be able to grow in absolute terms

- Longevity – the solution should remain contemporary for some years

- Resilience and security – EIE needs to be trusted

The EIE Infrastructure is intended to support many processes and functions. Of these, the two key functions are:

- Messaging – Transport of the messages that make up valid transactions and processes

- Bulk file transfer – Transport of larger existing and anticipated files not suited to messaging

The EIEnet solution has also been guided by the preference of the Architecture Working Committee for a decentralised peer to peer solution for EIE Infrastructure where possible.

Leveraging off prior experience

The most significant existing common network is that used for MNP. While the MNP Common Network meets many EIE requirements it was designed for specific types of Participants and does not cater for Participants with less complex needs and smaller volumes of transactions. The EIEnet is based on the good design laid down by MNP and also caters for Participants whose needs are different to encourage early actual usage of EIE by a wider variety of Participants.

Objectives to be Achieved

The EIEnet is intended to support:

- a wide range of connection methods to support various levels of activity for EIE processes;
- access to EIEnet for all relevant Participants such that no party is placed at a competitive disadvantage;
- growth in such a way as to facilitate and not hinder increased usage of EIE;
- an EIE Infrastructure that will be contemporary, accessible and sufficiently long lived to encourage business and technical adoption;
- messaging and bulk file transfer;
- independence of suppliers and transparency to any other EIE Participant; and
- an architecture and infrastructure that does not require centralised management.

EIE Participants

A number of different categories of organisations are likely to benefit from the EIEnet:

- **Industry Operators**

  Access Service Deliverers

  Carriage Service Providers

  Portability Service Suppliers

  Service Providers

  Wholesalers

  Retailers

- **Regulators and Regulatory bodies**

  ACIF

  ACCC

  ACA

- **Suppliers**

  Equipment

  Facilities

  Infrastructure

- **Developers**

Organisations can have access to the EIEnet when they participate in one or more EIE applications.

Anticipated Benefits to Consumers

By providing a common network infrastructure, the EIEnet will provide benefits to all consumers of telecommunication related industries by enabling:

- lower costs for transaction transport between Participants;
- shorter lead times to develop transport mechanisms and therefore faster time for application development to bring new products to market;
- data transfer with less errors as a result of the automated electronic exchange; and
- provide greater security over data being exchanged between Participants.

Anticipated Benefits to Industry

The communications industry operates within a diverse and complex process environment. The processes within this environment and the relationships between industry operators often require multiple links to various Participants for various applications.

The development of an EIEnet represents an opportunity to improve greatly the interactions between the industry operators by providing a single connection for a multiplicity of applications with various other Participants. The eventual migration of some applications that presently require dedicated links will also minimise costs for many EIE Participants.

The EIEnet forms the backbone method of facilitating delivery of transactions to other industry Participants allowing Participants to concentrate on the actual application development. By not having to reinvent new delivery mechanisms this makes it easier for industry to develop and deploy new products and applications.

Anticipated Cost to Industry

The communications industry operates within a diverse and complex process environment. The processes within this environment and the relationships between industry operators often require multiple links to various Participants for various applications.

The development of an EIEnet represents an opportunity to improve greatly the interactions between the industry operators by providing a single connection for a multiplicity of applications with various other Participants. The eventual migration of some applications that presently require dedicated links will also minimise costs for many EIE Participants.

The EIEnet forms the backbone method of facilitating delivery of transactions to other industry Participants allowing Participants to concentrate on the actual application development. By not having to reinvent new delivery mechanisms this makes it easier for industry to develop and deploy new products and applications.

Ownership

Ownership of the EIE Administration Node application software belongs with ACIF.

The EIEnet is a virtual network. Respective supplier(s) and EIE Participants will own the physical elements, but to ensure that no EIE application impacts on another application, access to the EIEnet will be under the control of the EIE Management Committee.

The owner(s) of the physical elements will have a number of responsibilities including security of access, transparency of interconnection, performance, reliability and change management. Implementation of relevant EIE applications will be the responsibility of the Participants.

Review

The Guideline was reviewed in late 2003 to standardise the use of terms used to identify EIEnet users, to allow the use of the same MNP PIPN infrastructure for EIE purposes (where approved by the EIEMC and the MNP Administration Group and subject to the effect that it has no impact on MNP performance) and includes checklists to assist users of the EIEnet.

Alexander R Osborne

Chairman

EIEMC/WG1: EIE Infrastructure Common Network Working Group

PARTICIPANTS

The Working Group responsible for the revisions made to the Guideline consisted of the following organisations and their representatives:

Organisation	**Representative**
AAPT	Peter McDonald
AAPT	Atul Sood
Comindico	Maree Mayo
Hutchison Telecoms	Alexander R. Osborne
Optus	Hari Ramachandran
Paradigm One	Devendra Gupta
Telstra	Dang Phan
Telstra	Patrick Kishta

The Working Group was chaired by Alexander R. Osborne. Margaret Fleming of ACIF provided project management support.

TABLE OF CONTENTS

1 SCOPE AND OBJECTIVES

1.1 Scope

This document specifies the requirements of the EIEnet to provide interconnectivity which facilitates electronic information exchange between Participants.

1.2 Objectives

The purpose of this document is to define technical specifications and other requirements for interfacing between Participants and the behaviour of a single and multiple provider EIEnet.

A multiple provider EIEnet must provide seamless and transparent interconnection between any and every EIE Participants.

1.3 Guideline review

Review of the Guideline will be conducted after 12 months of initial commencement and every five years subsequently.

2 ACRONYMS, DEFINITIONS AND INTERPRETATIONS

2.1 Acronyms

For the purposes of the Guideline, the following acronyms apply:

ATM	Asynchronous Transfer Mode
CA	Communications Alliance
BGP	Border Gateway Protocol
CSP	Carriage Service Provider
DNS	Domain Name Server
DSL	Digital Subscriber Line
EIE	Electronic Information Exchange
EIEMC	Electronic Information Exchange Management Committee
IP	Internet Protocol
IPsec	IP Security
ISDN	Integrated Service Digital Network
MNP	Mobile Number Portability
PIPN	Private IP Network
PSTN	Public switched telephone network
SLA	Service Level Agreement

2.2 Definitions

For the purposes of the Guideline, the following definitions apply:

Act

means the *Telecommunications Act 1997*.

Application Provider

means the entity providing an application deployed on the EIEnet.

Application User

means the entity using an application deployed on the EIEnet.

Carriage Service Provider

has the meaning given by section 87 of the *Act*.

Carrier

has the meaning given by section 7 of the *Act*.

DS3

means Digital Signal Level 3 digital signal transmission as 45 Mbps bit rate.

E1

means the label used to describe the digital signal transmission as 2 Mbps bit rate.

EIE Administration Node

means the central node that provides services to support applications deployed on the EIEnet.

EIEnet

means the EIE Common Network.

EIEnet Provider

means the Network Provider of the EIEnet.

Network Provider

means a supplier of the physical EIE network infrastructure.

Participant

means a party involved in EIE applications.

xDSL

means the family of digital subscriber line products.

2.3 Interpretations

In the Guideline, unless the contrary appears:

(a) a reference to a statute, ordinance, code or other law includes regulations and other instruments under it and consolidations, amendments, re-enactments or replacements of any of them;

(b) words in the singular includes the plural and vice versa;

(c) words importing persons include a body whether corporate, politic or otherwise;

(d) a reference to a person includes a reference to the person's executors, administrators, successors, officer, employee, volunteer, agent and/or subcontractor (including but not limited to, persons taking by novation) and assigns;

(e) if a period of time is specified and dates from a given day or the day of an act or event, it is to be calculated exclusive of that day; and;

(f) a reference to a day is to be interpreted as the period of time commencing at midnight and ending 24 hours later.

3 REFERENCES

Publication	Title
Industry Guidelines	
ACIF G573:2004	Mobile Number Portability IT Specification, Part 3: Common Network

Industry Documents	
EIE Architecture and Planning Phase - Infrastructure Architecture Issues and Requirements	
EIE Architecture and Planning Phase - Security Addendum to the Architecture Requirements	
EIE Architecture and Planning Phase - Final Report	
EIE Overview and Concepts	
Telecommunications Act 1997	

4 EIE COMMON NETWORK (*EIENET*)

4.1 Introduction

4.1.1 EIE infrastructure is an electronic Business-to-Business (*B2B*) messaging platform that allows Participants to exchange information electronically with each other, in order to perform business functions. The EIE infrastructure is designed to accommodate a large variety of business applications.

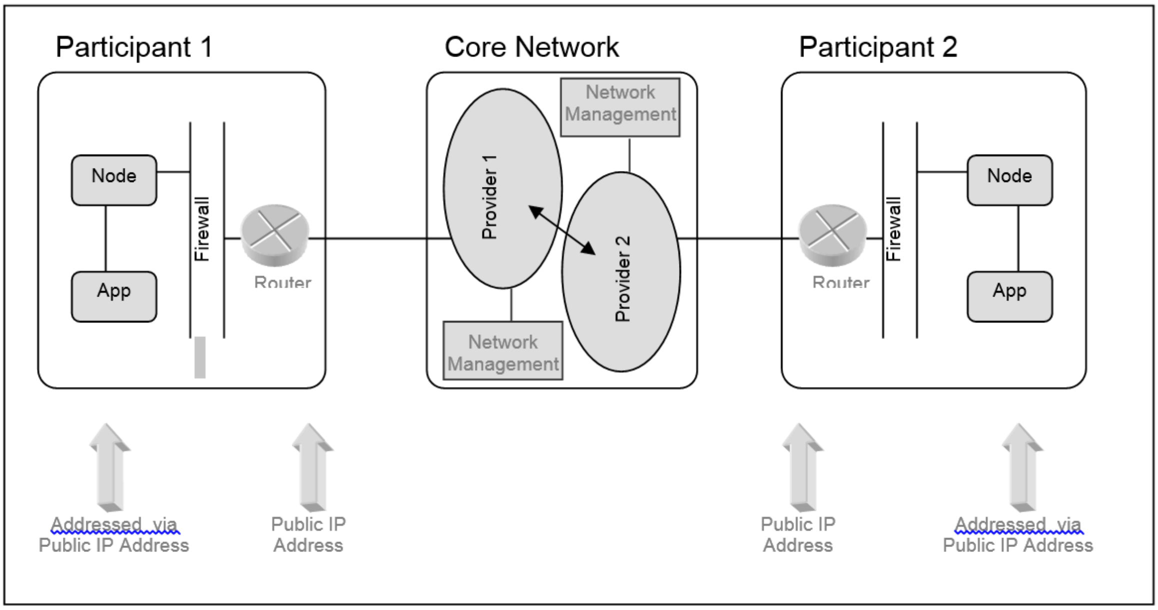


FIGURE 1

EIEnet – Conceptual View

4.1.2 The EIEnet will be provided by one or more Network Providers. A multiple-provider EIE Common Network will provide seamless and transparent interconnection between any and every EIE Participant. Network management is expected to be provided by each Network Provider.

4.1.3 Information exchange is essentially between peer-to-peer messaging nodes. Messaging nodes are connected through the EIEnet. Connection to the EIEnet will be via a supported dedicated access or dial-up access method.

4.1.4 Nodes will be connected to the EIEnet via Participant supplied equipment (i.e. routers) and are protected by firewalls and other relevant security provisions. Each node must be addressable via a public IP address.

4.2 Access

4.2.1 The EIEnet is a communications medium that is only available to those parties approved by the EIEMC for EIE approved applications.

4.2.2 ElEnet Providers must not provide access to the ElEnet without the written consent of the EIEMC.

4.2.3 The ElEnet will support both dedicated and dial-up access.

4.2.3.1 Dedicated access will support one or more of the following technologies:

(a) ATM

(b) Frame Relay

(c) E1

(d) DS3

4.2.3.2 Dial-up access will support one or more of the following technologies:

(a) Internet access

(b) xDSL access

(c) Service Provider solutions (PSTN, ISDN)

(d) Cable modems

NOTE: Applications will determine whether dial-up access is supported.

Detailed requirements for the access technologies are specified in the following table.

TABLE 1

Access Specification

Access Technology	Connection Protocol	Authentication Protocol	IP Address	Routing Protocols	Potential Speeds to be supported
ATM	ATM-UNI 3.1	N/A	Public	BGP4, Static	16Kbps to 34Mbps
Frame Relay	V.35, X.21, G.704	N/A	Public	BGP4, Static	16Kbps to 34Mbps
E1	E1	N/A	Public	BGP4, Static	2Mbps
DS3	DS3	N/A	Public	BGP4, Static	45Mbps
Internet access	PPP	RADIUS & IPsec	Public	Static	56Kbps to 128Kbps
XDSL access	PPP	RADIUS	Public	Static	64Kbps to 1.5Mbps
SP Solutions	PPP	RADIUS	Public	Static	56Kbps to 128Kbps
Cable modems	PPP	RADIUS	Public	Static	Up to 10Mbps

NOTE: The parameters used in the authentication of a dial-up access must, as a minimum, include the ability to track a user name to a valid access organisation (Network Provider). For example, ensuring a User Name contains a registered internet domain name (e.g. joe.bloggs@mysp.com.au).

The internet access must be secured with an encrypted IPsec tunnel. X.509 digital certificate or IPsec shared secret, IKE protocol, and Triple-DES with 128-bit encryption must be used with the establishment of an IPsec tunnel.

Network Providers must apply firewall policies to permit packets only with a valid source address for the IP address range defined for each access connection. Additional firewall security must be applied for each internet access to deny packets that bear a source address used with other access methods.

4.3 EIEnet Access Technologies

4.3.1 Various permutations of EIEnet access technology are shown in the following diagrams.

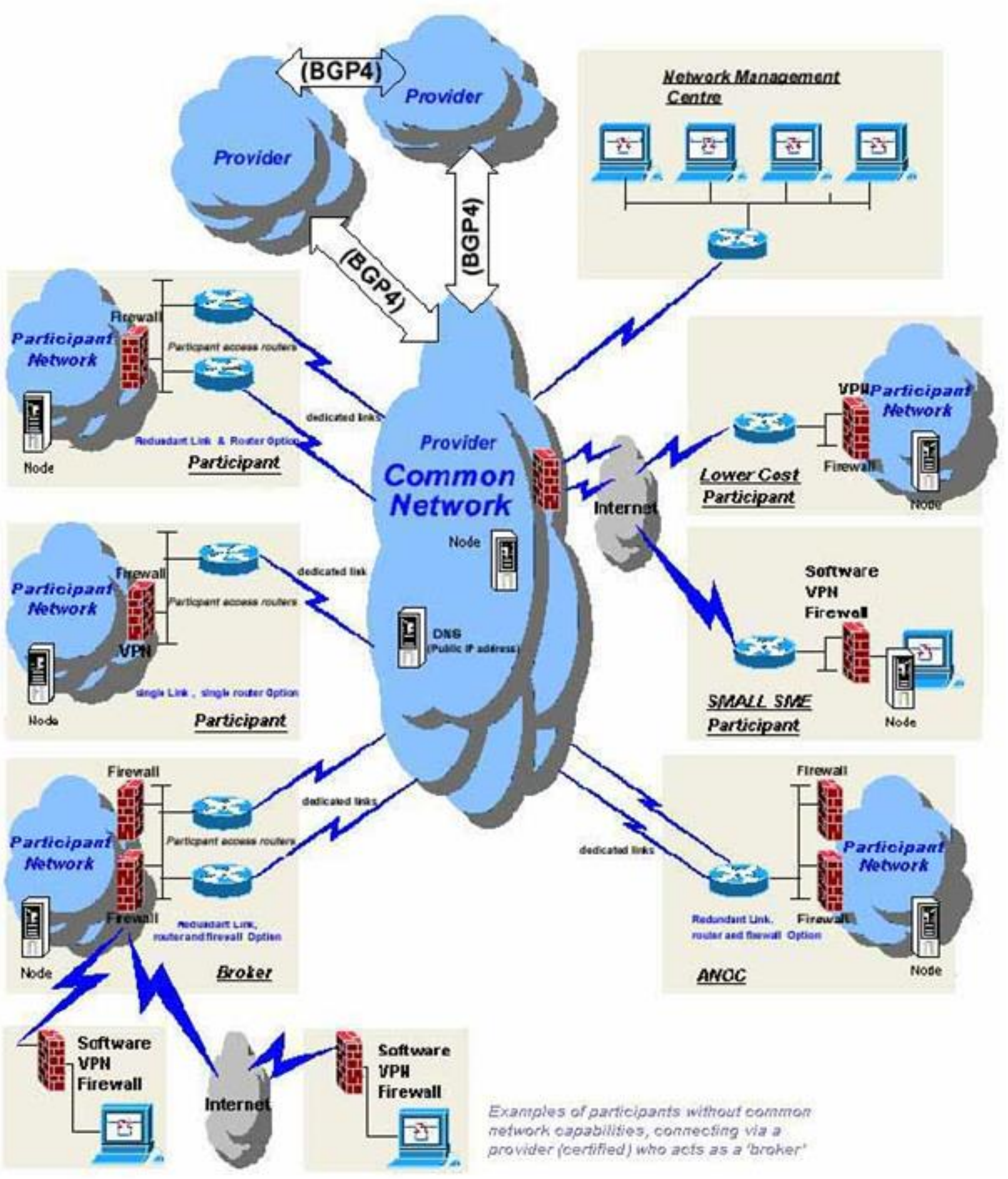


FIGURE 2

EIEnet with access permutations

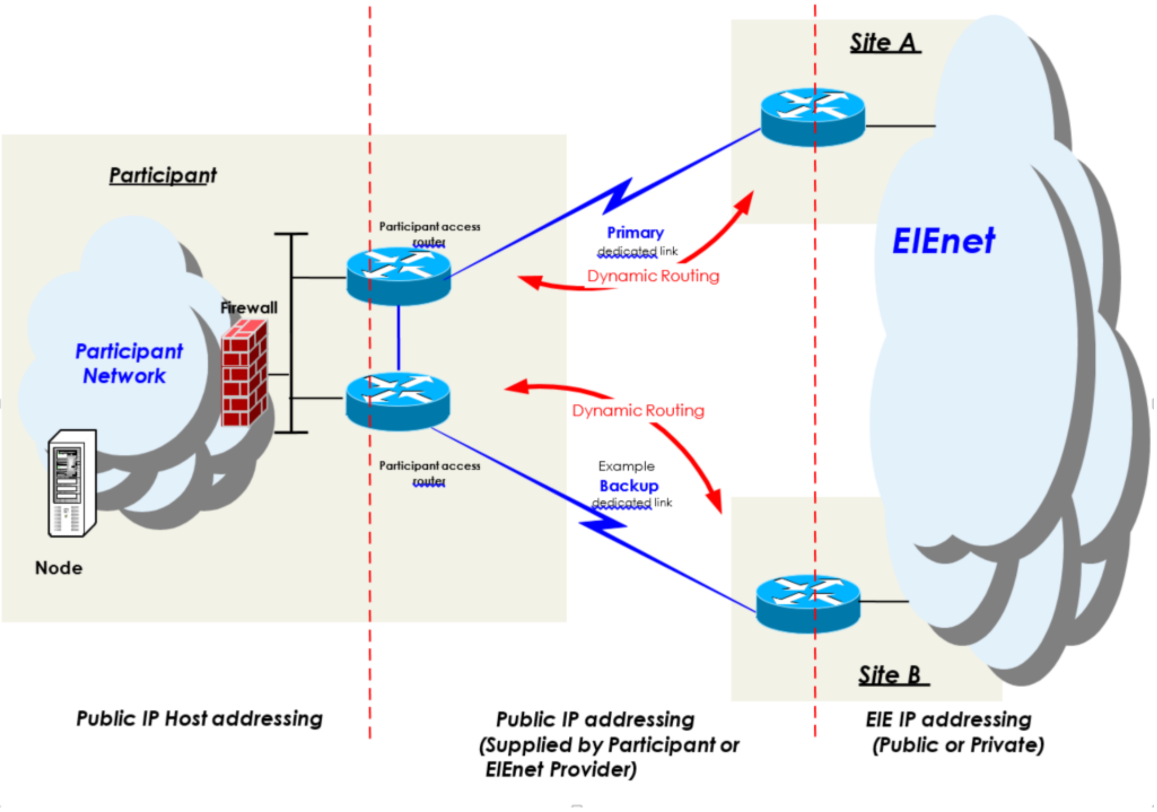

Site A
Participant
Participant access router
Primary
dedicated link
Dynamic Routing
ElEnet
Firewall
Participant Network
Dynamic Routing
Participant access router
Example
Backup
dedicated link
Node
Site B
Public IP Host addressing
Public IP addressing (Supplied by Participant or ElEnet Provider)
EIE IP addressing (Public or Private)

FIGURE 3

Example of access to ElEnet with dynamic routing

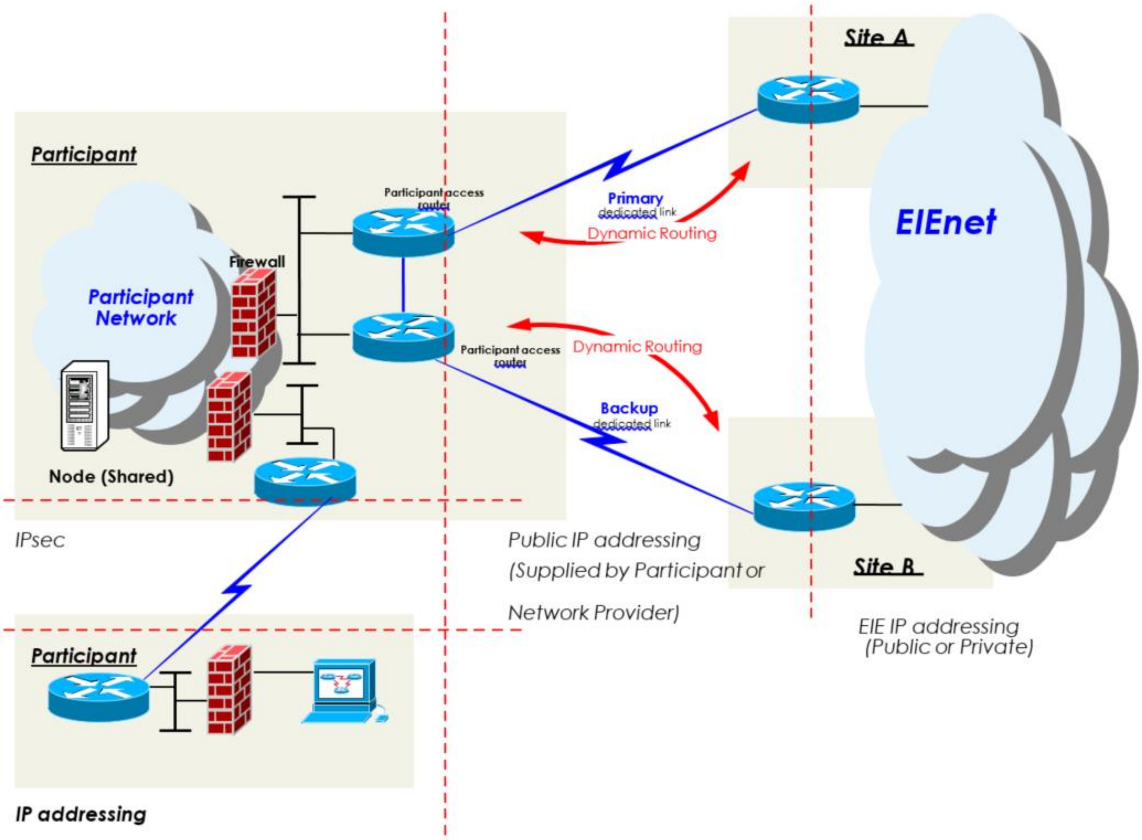


FIGURE 4

Example of a certified EIE Participant providing a bureau service

4.4 Interconnection

4.4.1 Network Provider to Network Provider

4.4.1.1 Border Gateway Protocol (BGP4) must be used as the base routing protocol for interconnection between Network Providers.

4.4.2 Participant to Network Provider

4.4.2.1 A Participant will access the EIEnet through the network access device (e.g. router) located on the Participant's premise. The network access device can be managed either by the EIEnet Provider or by the Participant.

4.4.2.2 If using a router, the Participant may elect to use static or dynamic routing between themselves and the EIEnet dependent on their choice of access and application.

4.4.2.3 It is highly recommended that Border Gateway Protocol (BGP4) is used as the base routing protocol for interconnection between the Participant and Network Provider where dynamic routing protocol is required.

4.4.2.4 For maximum compatibility, proprietary network routing protocols (for example, IGRP, EIGRP) must not be used.

4.4.3 Priority Scheme

4.4.3.1 A priority scheme is a term that refers to a traffic path associated with a data traffic priority. A minimum of two priority schemes must be supported by the Network Provider. This is to facilitate separation of applications with different data traffic priorities (e.g. test and production).

4.4.3.2 The implementation of the priority scheme will be negotiated between the Participant and the Network Provider.

4.4.3.3 Where a Participant uses the MNP PIPN as the EIEnet, each application associated with the EIEnet as authorised in Clause 5.1 of ACIF G573.3:2004 Mobile Number Portability IT Specification, Part 3: Common Network Industry Guideline must be on a channel separate to those used for MNP, and must not have any impact on any MNP channel or priority scheme

4.5 IP Addressing

4.5.1 EIE application servers and Participant access routers must be addressable using public IP addresses. Where the Participant does not supply the Public IP addresses then they may be supplied by the Network Provider.

4.5.2 Within the EIEnet, public or private IP addresses may be used.

4.5.3 IP v4 is the protocol to be used.

4.6 Setup of Firewall

4.6.1 A firewall must be used in the Participant network. The firewall must be capable of passing authorised inbound and outbound traffic of relevant EIE applications.

4.7 Domain Name System (DNS)

4.7.1 A Network Provider may provide a DNS service for use by the EIE Participants. Where the DNS service is provided it must be accessible using a public IP address.

4.8 Network Security between the Participant and Network Provider

4.8.1 Dial-up Access

4.8.1.1 IP tunnels are to be used over internet connections. The security method to be used is IPsec. It is highly recommended that IPsec client software supplied will conform to Internet Engineering Task Force (IETF) IPsec Working Group RFCs.

4.8.1.2 The parameters used in the authentication of a dial-up access must, as a minimum, include the ability to track a user name to a valid access a User Name containing a registered internet domain name (*e.g. joe.bloggs@mysp.com.au*) and a password.

4.8.1.3 The internet access must be secured with an encrypted IPsec tunnel. X.509 digital certificate or IPsec shared secret, IKE protocol, and Triple-DES with 128-bit encryption must be used with the establishment of an IPsec tunnel.

4.8.1.4 Network Providers must apply firewall policies to permit packets only with a valid source address for the IP address range defined for each access connection. Additional firewall security must be applied for each internet access to deny packets that bear a source address used with other access methods.

4.8.2 Wireless Access

4.8.2.1 If access is wireless, the Network Provider must demonstrate that the wireless network is secure. Encryption provided from the device to the network must meet or exceed the same level of security as specified for dial-up access over the internet.

4.9 Network Scalability

4.9.1 The network solution must be scalable to be able to carry actual volumes of EIE transactions. It is expected that each Network Provider has monitoring and upgrade capabilities to ensure that their network can meet the demand.

5 DATA LINK REDUNDANCY

5.1 Participant

5.1.1 It is highly recommended that Participants subscribe to a back-up link to an alternative physical path. This is to be addressed through commercial agreement between each Participant and a nominated Network Provider.

5.1.2 Participants may arrange back-up links in two ways:

(a) by subscribing to multiple Network Providers (where available); or

(b) by having fully redundant (and, where possible, diversely routed) links to different locations of a single Network Provider.

5.2 Network Provider

5.2.1 The Network Providers must ensure their networks have no single point of failure and must be able to support requirements for back-up links with location diversity.

5.2.2 It is the responsibility of the Network Provider to meet minimum SLAs as specified in Section 6 of this document and relevant application specific SLAs.

6 SERVICE LEVELS

6.1 Core Network Availability

6.1.1 The standard availability target for all EIE Network Providers is 99.85%.

6.1.2 The service performance objectives in Table 2 apply to EIE Network Providers.

TABLE 2

Service Performance Objectives

Class of Service	**Standard**
Data Delivery Ratio %	99.90%
Frame Relay	V.35, X.21, G.704
Network Availability %	99.98%
Round Trip Transit Delay (milliseconds maximum)	100
Packet Delay Variation (milliseconds maximum)	20

6.1.3 Availability targets are averaged over a one calendar month period. All targets apply within the EIEnet and do not include access services. Planned outages are excepted Notification of Readiness.

NOTE: The above figures do not include access points.

6.2 Planned Outages

6.2.1 In the event that a Network Provider needs to carry out maintenance on their network, they must notify CA, each of their Participant customers and other Network Providers as per pre-established bilateral arrangements. Should maintenance require industry co-ordination with respect to scheduling the planned outage, agreement must be sought through the EIE Management Committee and agreement must be in place before the planned outage is carried out.

6.2.2 Details of all planned outages will be provided on the CA website and updated when there is a change.

6.2.3 CA will maintain the planned outages log on their website – www.commsalliance.com.au with updates on a daily basis or within 24 hours (1 business day) of notification of the outage. The planned outage log is password protected.

7 COMMERCIAL OFFERING

Access to the EIEnet will be provided to Participants by Network Providers on a commercial basis.

8 FAULT MANAGEMENT

8.1 General

8.1.1 The EIEnet must provide self-diagnostic capability to identify faults in the network. The self-diagnostic capability includes the ability for any Participant to 'ping' and 'trace-route' to all other Participants' access routers and edge routers across different EIEnet physical networks.

8.1.2 A contact list must be provided to CA by each EIEnet Provider for the reporting and escalation of faults. The list must include first, second and third level contact details. The contact list will be available to EIEnet Participants on the CA website.

8.1.3 Fault management procedures and Service Levels must be agreed between the Participant and the EIEnet Provider.

8.2 Participant to EIEnet Provider

8.2.1 EIEnet Participants and Provider(s) are responsible for ensuring that appropriate arrangements are agreed between themselves for fault management procedures.

APPENDIX

A EIE APPLICATION PROVIDER CHECKLIST

For applications enabling peer to peer communications

An Application provider is required to go through the following steps to arrange connection to the EIEnet and use of an application on the EIEnet.

1. CA

1.1 If not currently an EIE Subscriber, approach the CA EIEMC for approval to subscribe to the EIE.

1.2 If a current EIE Subscriber go to next step.

Description	The Application Provider's organisation must be an EIE contracted subscriber. This is the "*financial*" subscription where the organisation pays its dues.
Rationale	Without being a subscriber, access to EIE will not be given by CA.
Cost	EIE membership fees are incurred. No system cost impact.
Reference Documentation	EIE Overview and Concepts EIE Subscriber Agreement

1.3 Approach the CA EIEMC for approval to deploy the application on the EIEnet.

1.4 Where the Application Developers request to deploy the application on the EIEnet is approved, the EIEMC to authorise the EIEnet Provider(s) to implement an application access connection within the EIEnet.

> *NOTE: The new application access connection must not impact the existing applications if an existing channel is shared. The network solution provider and the Application Provider and Application User will determine the optimum solution for application access connection.*

2. Administration Node Operating Company (ANOC)

2.1 Approach the ANOC to arrange:

- EIE Subscription

Description	The Application Provider's organisation must be registered upon the EIE Administration Node. This is the 'physical' subscription where the organisation is assigned a user ID and password.
Rationale	Without system registration an organisation and its staff cannot access the EIE Administration Node and utilise its components.

Cost No further system cost impact to deploy the application.

However, cost will be incurred for any specific application development required to support the application in the EIE Administration Node (e.g. specialised screens).

Reference Documentation Application provider can confirm registration through EIE web portal subscriber administration details.

- Loading of application service definitions into the "centralised register and repository"
- Development of test scenarios for "compliance checking" (optional) where it is requested by the Application Provider.

3. EIEnet Provider

3.1 Approach EIEnet Provider(s) to discuss the impact of the new application; including identifying target audience and size and volume of transactions; to determine most appropriate EIEnet access solution, then:

- if no link in place, arrange EIEnet connection; or
- if link in place, review current bandwidth and assess need for additional bandwidth;
- identify approach to either sharing a channel, or adding an additional channel for the new application

Description Where approval given by the EIEMC to deploy an application on the EIEnet:

- CA EIEMC to authorise the EIEnet Provider to implement an application access connection within the EIEnet.
- The Application Provider to determine with the EIEnet Provider and the Application User the optimum solution for application access connection.

NOTE: The new application access connection must not impact any existing applications, especially where an existing channel is shared.

Rationale To ensure that access to existing applications over the EIEnet is not adversely impacted.

Cost Network dollars will be incurred by the Application Provider and/or Application Users if new network connection or additional bandwidth on an existing network connection is required. The magnitude of the cost will vary, depending on the solution determined for the specific application.

Reference Documentation G608:2004 **EIE Infrastructure Common Network Specification** Industry Guideline.

4. Application Provider to ensure:

4.1 Applications using WSDL must be compliant with Web Services International Standards.

Description This can be done by utilising the EIE Administration Node's WSDL compliance checker.

Rationale This is the only way to ensure full interoperability across any to any platform communication.

Cost No cost to provide ability to access the International Web Services Standards body for WSDL standard compliance checking and functionality is fully re-useable.

Reference Documentation ws-i.com website

(http://www.ws-i.org/implementation.aspx) will be used.

4.2 The Application Provider must arrange with the ANOC to ensure that the appropriate WSDL is loaded into the "centralised register and repository".

Description The EIE Administration Node must be enabled to extract and download the WSDL from the Application Provider's storage source.

The EIE Administration Node will support multiple versions of the WSDL documents.

The EIE Administration Node has the ability to:

- provide a Polling and synchronisation mechanism between the EIE Administration Node and the Application Provider's document source
- notify subscribers of service definition changes
- display registered service definitions for viewing by subscribers

Rationale Ensure any organisation can view application service definitions (WSDL and associated content).

Cost Any costs associated with the development of specific screens required for an application are the responsibility of the Application Provider.

Reference Documentation Centralised registry and repository is accessible through: https://prod.eie.net.au/portal

4.3 Compliance checking must be available on the EIE Administration Node.

Description

Application Provider is to provide the appropriate documentation that will enable application level compliance checking to be performed by the EIE Administration Node:

- WSDLs
- transaction dialogues
- test scenarios that meet compliance criteria

Application Provider must request a new Application User to undertake compliance checking against the EIE Administration Node. Upon successful completion of compliance checking by the Application User, the ANOC must send e-mail notification to the Application Provider and Application User, including compliance checker logs. The Application Provider must obtain this notification in relation to an Application User before allowing that Application user access to the application.

The EIE Administration Node will support the testing of multiple releases.

Where an existing application is being made available via the EIEnet the Application Provider may waive compliance testing against the EIEnet Administration Node by the Application User, and in this case will provide the certificate of compliance to the Application User itself.

Rationale

Enables shake out of potential system issues.

Enables any valid customer to commence development without having to be scheduled into an Application Provider's deployment schedule.

Compliance checking on the EIE Administration Node is always available (as per the contractual SLA's between ANOC and CA), i.e. no dependency on the Application Provider.

Enables a much smoother transition into integration testing with the Application Provider.

Cost

Any costs associated with development or deployment of required test scenarios for the EIE Administration Node are the responsibility of the Application Provider.

Reference Documentation

EIE Administration Node Core Services
EIE Compliance Checking – Application Provider Template

APPENDIX

B EIE APPLICATION USER CHECKLIST

For applications enabling peer to peer communications

On approval from an Application Provider to allow access to an application deployed over the EIEnet, the Application User is required to go through the following steps to arrange connection to the EIEnet:

1. CA

1.1 If not currently an EIE Subscriber, approach the CA EIEMC to subscribe to the EIE.

1.2 If a current EIE Subscriber go to step 2.

Description The Application User's organisation must be an EIE contracted subscriber. This is the "*financial*" subscription where the organisation pays its dues.

Rationale Without being a subscriber, access to EIE will not be given by CA.

Cost EIE membership fees are incurred.

No system cost impact.

Reference Documentation EIE Overview and Concepts

EIE Subscriber Agreement

2. Administration Node Operating Company (ANOC)

2.1 Approach the ANOC to register subscription to the EIE and to use application(s) deployed on the EIEnet:

Description The Application User's organisation must be registered upon the EIE Administration Node. This is the 'physical' subscription where the organisation is assigned a user ID and password.

Rationale Without system registration an organisation and its staff cannot access the EIE Administration Node and utilise its components.

Cost No further CA cost to access the deployed application.

However, costs are likely to be incurred to access any specific applications, payable to the Application Provider.

Reference Documentation Application provider can confirm registration through EIE web portal subscriber administrator details.

3. EIEnet Provider

3.1 Approach EIEnet Provider(s) to discuss the impact of accessing the application; including size and volume of transactions, to determine most appropriate EIEnet access solution, then:

- if no link in place, arrange EIEnet connection; or
- if link in place, review current bandwidth and assess need for additional bandwidth;
- identify approach to either sharing a channel, or adding an additional channel for the new application

Description

Where the Application User has subscribed to EIE and approval given by the Application Provider to access a deployed application on the EIEnet the Application User to determine with the EIEnet Provider and the Application Provider the optimum solution for application access connection

NOTE: The new application access connection must not impact any existing applications, especially where an existing channel is shared.

Rationale

To ensure that access to existing applications over the EIEnet is not adversely impacted.

Cost

The Application User will incur network dollars if new network connection or additional bandwidth on an existing network connection is required. The magnitude of the cost will vary, depending on the solution determined for the specific application.

Reference Documentation

G608:2004 **EIE Infrastructure Common Network Specification** Industry Guideline.

4. Application User to ensure:

4.1 The appropriate WSDL is loaded from the “centralised register and repository” (where applicable).

Description

The EIE Administration Node must be enabled to extract and download the WSDL from the Application Provider’s storage source.

The EIE Administration Node will support multiple versions of the WSDL documents.

The EIE Administration Node has the ability to:

- provide a Polling and synchronisation mechanism between the EIE Administration Node and the Application Provider’s document source
- notify subscribers of service definition changes

display registered service definitions for viewing by subscribers

Rationale Ensure any organisation can view application service definitions (WSDL and associated content).

Cost Any costs associated with the development of specific screens required for an application are the responsibility of the Application Provider

Reference Documentation Centralised registry and repository is accessible through: https://prod.eie.net.au/portal

4.2 Compliance checking carried out on the EIE Administration Node.

Description Application User to access appropriate documentation to carry out application level compliance checking to be performed by the EIE Administration Node:

- WSDLs
- transaction dialogues
- test scenarios that meet compliance criteria

Upon successful completion of compliance checking, the ANOC must send e-mail notification to the Application Provider and Application User, including compliance checker logs. The Application Provider must obtain this notification in relation to the Application User before allowing that Application User access to the application.

NOTE: The EIE Administration Node will support the testing of multiple releases.

Rationale Enables shake out of potential system issues.

Enables any valid customer to commence development without having to be scheduled into an Application Provider’s deployment schedule.

Compliance checking on the EIE Administration Node is always available (as per the contractual SLA’s between ANOC and CA), i.e. no dependency on the Application Provider.

Enables a much smoother transition into integration testing with the Application Provider.

Cost Any costs associated with completing the required test scenarios for the EIE Administration Node are the responsibility of the Application Provider.

Reference Documentation EIE Administration Node Core Services
EIE Compliance Checking – Application Provider Template

Communications Alliance was formed in 1997 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services.

In pursuing its goals, Communications Alliance offers a forum for the industry to make coherent and constructive contributions to policy development and debate.

Communications Alliance seeks to facilitate open, effective and ethical competition between service providers while ensuring efficient, safe operation of networks, the provision of innovative services and the enhancement of consumer outcomes.

It is committed to the achievement of the policy objective of the *Telecommunications Act 1997* - the greatest practicable use of industry self-regulation without imposing undue financial and administrative burdens on industry.

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507

Care should be taken to ensure the material used is from the current version of the Standard or Industry Code and that it is updated whenever the Standard or Code is amended or revised. The number and date of the Standard or Code should therefore be clearly identified. If in doubt please contact Communications Alliance