ABFAB
Internet-Draft
Intended status: Informational
Expires: September 13, 2012

Y. Wei, Ed.
ZTE Corporation

March 12, 2012

Federated Cross-Layer Access
draft-wei-abfab-fcla-02

Abstract

Network stratum and application stratum form a federation to faciliate user's access. Network operator acts as Identity Provider (IdP), and application reuses underlying network's security capabilities to simlify application's access. This document is to introduce such federated cross-layer access use case and message flows.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 13, 2012.

Copyright Notice

Table of Contents

1. Introduction

Currently it is agreed that digital identity is a crucial element in a service enviroment. Typically telecom operators provide access customers with identity which is associated with some form of trusted element on the network (e.g. SIM/UICC). Meanwhile the identity required by Web or non-Web services for users on is usually associated with username.

Ordinarly telecom operators have tens of millons of users and can provide trusted identity and higher security. However the categories of service provided by telecom operators are relatively few. On the contrary most service providers on the Internet have limited amount of users and can not assure the security of user identity, but they can provide abundant kinds of service. Furthermore, user is reluntant to register too many accounts because it is inconvenient to remember dozens of passwords . These facts creates some driving forces that telecom is interworking with Internet. The stakeholders can benifit from these combination. For telecom operators, they can provide identity service, trusted security service, mobile payment service and sharing some user profiles according user's preferences. Telecom operators is not just providing pipeine for communication, but also become a part of service value chain. For service providers, they can focus on core business and reuse capabilities provided by telecom operators without worring about sources of users. For end users, they can enjoy seamless service experiences and improve security and privacy.

This document considers a use case which telecom operator acts as Identity provider (IdP) and federates with non-Web applications, e.g. Email, Messaging. This use case combines network stratum access and application stratum access, which is named as federated cross-layer access. The detailed message flows for this use case are given.

2. Related Work

GSMA Association IDM project address operators' requirements for emerging mobile application (such as, Single Sign-on, mobile payments and other UICC enabled applications). Several use cases are also identified[GSMA_IDM]. Liberty Alliance Telecommunications SIG investigates digital identity grown in both telecom and Internet, develops several use cases and proposes correspoding solutions for interworking these two different domains [TelecoSiG].

GBA (Generic Bootsrapping Authentication) mechanism for boostrapping authentication and key agreement for application is denfined in [TS33.220]. The interworking between GBA and Identity Federation

Framework (ID-FE) is documented in [TR33.980]. Another interworking case between GBA and OpenID is specified in [TR33.924].

Currently some use cases [I-D.ietf-abfab-usecases], architecture [I-D.ietf-abfab-arch] and mechanisms are developed in IETF abfab working group.

3. Use Case

Editor's Note: The section is for readable and completeness for this memo. The formal use case is referred to [I-D.ietf-abfab-usecases].

Telecom operators have a communication network infrastructures to provider users with a wealthy of access methods. Telecom operators have a huge number of registered users, and they can provide trusted identity and higher security. Therefore they have a natural advantage to act as an Identity Provider (IdP) to serve for service providers. On the contrary most service providers on the Internet have limited amount of users and can not assure the security of user identity, but they can provide abundant kinds of service. Furthermore, user is reluctant to register too many accounts because it is inconvenient to remember dozens of passwords.

Telecom network supports Web or non-Web application. In some cases user prefers to choose non-Web application, e.g. Messaging service, VoIP, EMail service, etc. Based on the result of network stratum authentication and authorization, User equipment (UE) can access applications without doing another authentication and authorization

procedure. In this way, the system can implement federated cross-layer access. Firstly mutual authentication is performed between UE and Network, secondly UE accesses Application based on the result of network stratum's authentication. In this case, a federation is formed between Network and Application.

For federated cross-layer access, Network can assure the Application of the authenticity of user's identity, share some of use profile with Application. These can bring some benifits to stakeholders:

- For telecom operators, it becomes part of the business value chain as an Identity Provider.
- For service provider, it can focus on core competitive services without worrying about the number of registered users by reusing underlying security mechanisms during network stratum access.
- For end users, seamless sevice is provided, security and privacy are improved.

4. Message Flow

Take mobile network for example, UE has pre-shared key (PSK) with HSS. UE is mutully authenticated with network during attach procedure. After authentication, a master session key (MSK) is created on both UE and AAA. EAP [RFC3748] can enable the above procedure.

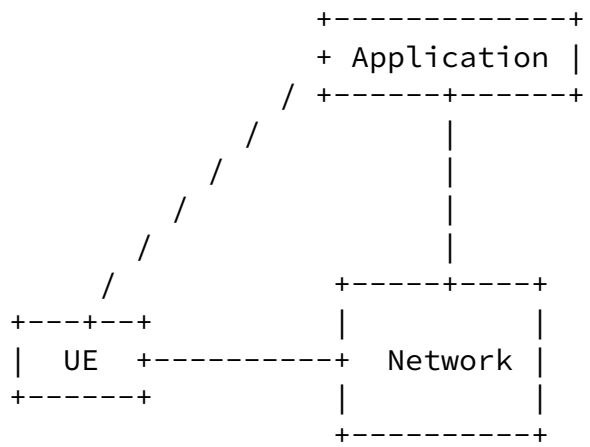


Figure 1: Federated Cross-Layer Access

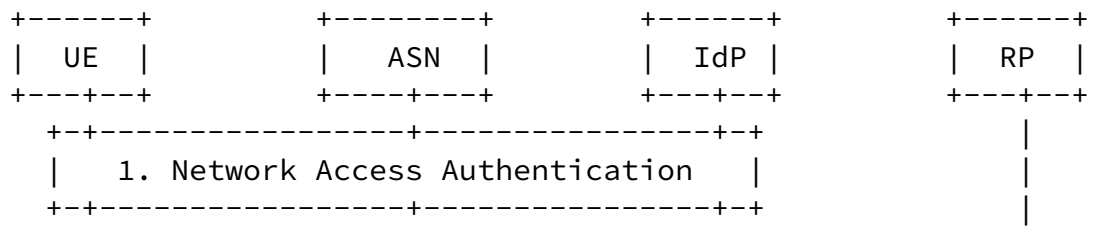
Figure 1 shows the relation among UE, network and application. Firstly mutual authentication is performed between UE and Network, secondly UE accesses Application using Single Sign-ON (SSO) based on network stratum's authentication. In this case, a federation is formed between Network and Application. The brief steps are as follows:

1. When UE attach the Network, mutual authentication is performed master session key is created between them.
2. UE visits non-Web Application, e.g Messageing service, VoIP service, or Email service.
3. Application has no information about the UE. The Application contacts Network to validate the authentication result in the network stratum. Application can find Network according the configuration or dynamical discovery protocol.
4. Network responds to Application with authentication result.
5. UE is authorized to access the Application.

4.1. Fast Re-authentication

The message flows below make use of the security capabilities provided by network and some building blocks, such as GSS-EAP [I-D.ietf-abfab-gss-eap], AAA-SAML etc.

As descirbed in the specification of GSS-EAP[I-D.ietf-abfab-gss-eap], UE maps onto GSS-API initiator, RP acts as GSS-API acceptor or EAP path-through authenticator, IdP maps onto EAP server. For the EAP is widely been used, this memo assumes the network access authentication is based on EAP. When UE visits application, it will improve the efficiency of authentication if the previous authentication result is reused. This procedure is called fast re-authentication, which is similar to the definition in EAP-AKA[RFC4187].



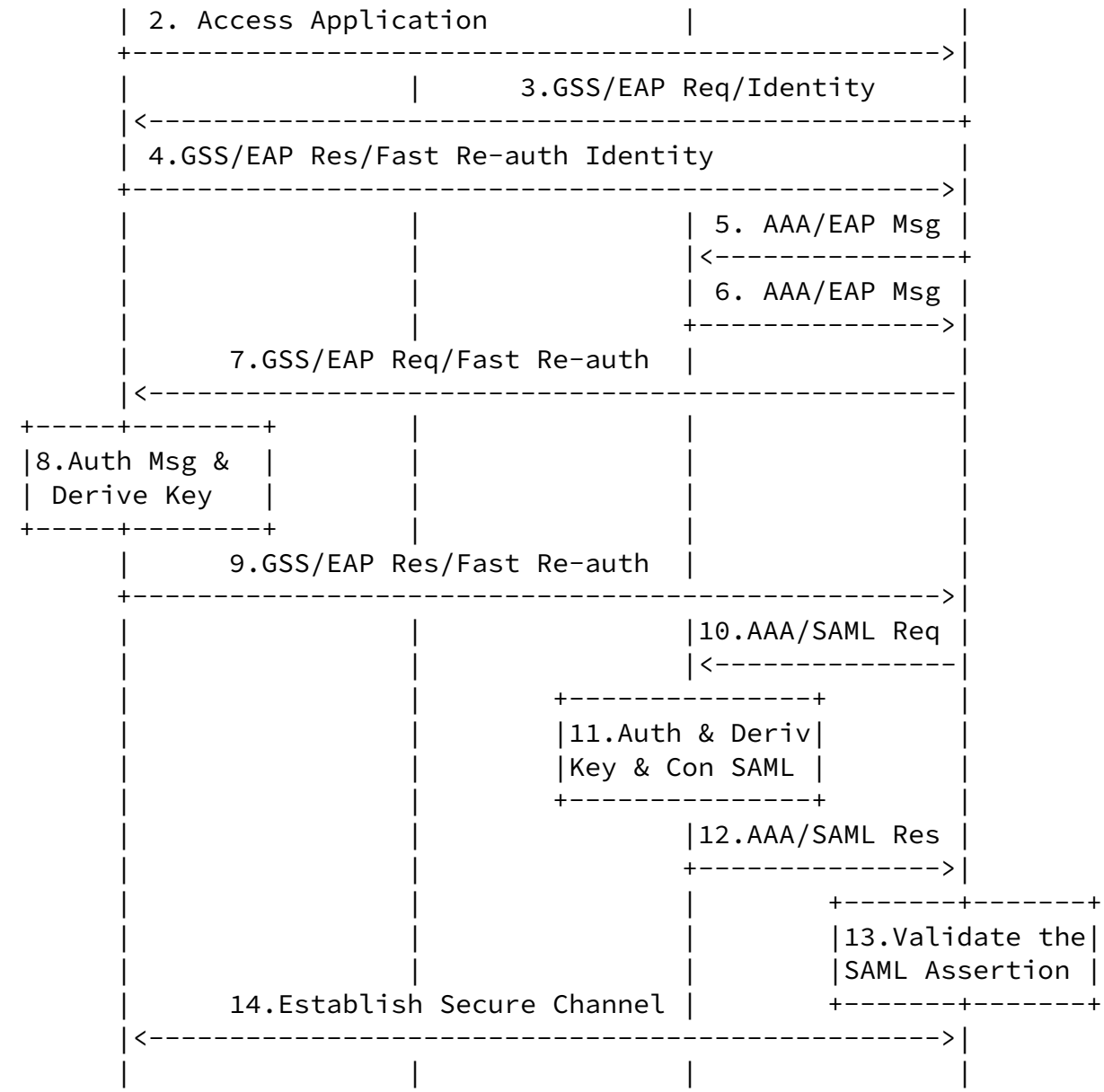


Figure 2: Fast Re-authentication

1. When UE access network, UE is performed mutual authentication with network. EAP can be utilized to facilitate the authentication procedure. EAP-Identity and EAP-Method will be exchanged between UE and network element. After successful authentication, an shared MSK is generated and stored in UE and IdP respectively, which can be used to authenticate other

applications and then establish secure channels. The network access authentication and key agreement is used as underlying security mechanism for GSS-API. The required credential for application is retrieved using gss_acquire_cred().

2. UE accesses Relying Party (RP). UE is identified by NAI [RFC4282]. GSS-API [RFC4121] is acted as underlying transport mechanisms.
3. RP responds with EAP Request/Identity message, which is contained in GSS-API token as a subtoken.
4. UE sends EAP Response/Identity message in GSS-API token, which may include fast re-authentication identity.
5. When RP receieves the request from UE, RP transfers the EAP message to IdP in AAA message. IdP checks the EAP message and agrees on fast re-authentication with UE.
6. IdP sends EAP-Request/Re-authentication to RP via AAA message.
7. RP strips off the AAA header and transfers the EAP message to UE via GSS-API token.
8. UE verifies the EAP message, thus authenticate the IdP using the credential retrieve from underlying security mechanisms. UE derives session key from previous credential, which will provide per-message protection, e.g. integrity protection, encryption.
9. UE sends EAP-Response/Fast Re-authentication message to RP using GSS-API token.
10. RP transfers the EAP message to IdP using AAA message with a SAML Request (samlp:AuthenRequest) [I-D.ietf-abfab-aaa-saml] [I-D.jones-diameter-abfab].
11. When the fast re-authentication is successful, IdP derives the same session key and constructs a SAML respone (samlp: AuthenResponse).
12. IdP sends the SAML response message to RP via AAA message.
13. RP validates the assertion in the SAML message. RP grants or denies access to the UE.
14. RP establishes secure channel with UE by means of GSS-EAP, thus the security services are also provided for message between UE and RP using gss_get_mic() and gss_get_warp().

4.2. Secure Data Sharing

After successful authentication, in order to provide effective services to customers, RP may need to retrieve some information from

operator's network, which stores some useful information (user

profile, contact list, and other resources etc.).

The following figure illustrate an arhchitecture of secure data sharingin for federated cross layer access. Network layer includes ASN, IdP and RS, which provides RP in application layer with secure services such as authentication and data sharing.

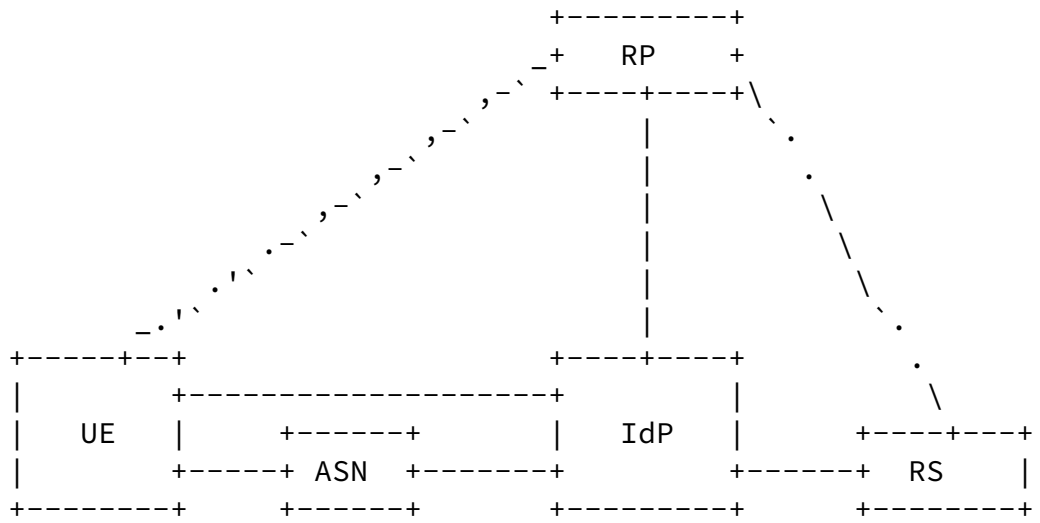


Figure 3: Architecture of Secure Data Sharing

- UE - User Equipment, it is identified by NAI and preconfigured with security credential.
- ASN - Access Serving Node, it is located at the border of network. It provides network access and authentication service to UE.
- IdP - Identity Provider, it is responsible for management of user identity. It provides authentication service to UE or RP. It is also to retrieve user information from RS and to provide them to RP in the condition of user's permission.
- RS - Resource Server, it stores user personal information, such as name, telephone, hobby, contact list, etc.
- RP - Relying Party, it provides user with such services as message service, VoIP, EMail service, etc.

The following figure depicts the procedure for secure data sharing. UE and IdP are mutually authenticated. RP reuses the authentication result in network access. RP may securely acquire user shared data with the authorization of the user.

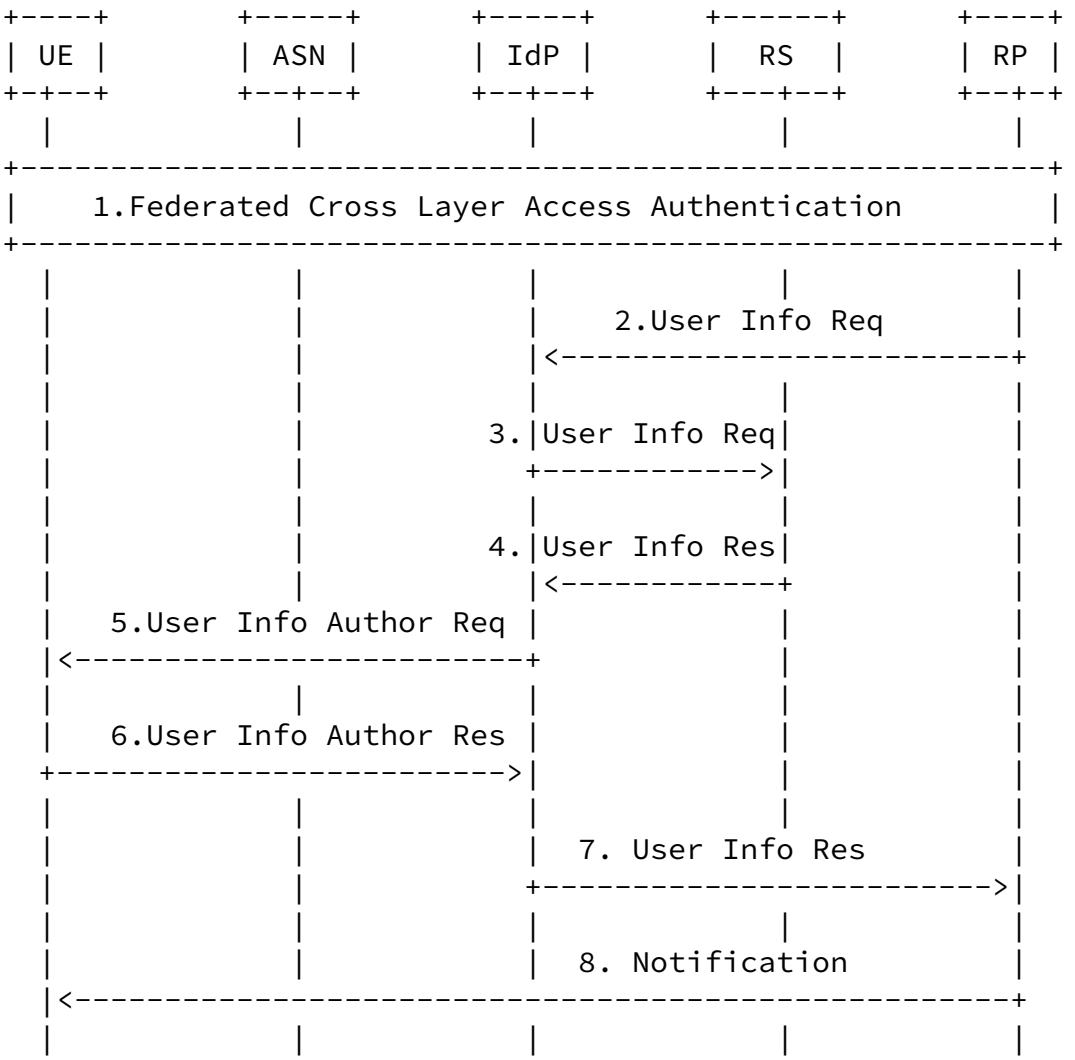


Figure 4: Procedure of Secure Data Sharing

1. UE performs federated cross layer access with IdP and RP, as shown in Figure 2.
2. When RP needs to acquire user's infomation for some services, RP sends user information request to IdP.
3. IdP verifies the request and sends user information request to RS.
4. RS validates the request and sends user information response to IdP according to the user's preferences.
5. IdP sends user information authorization request to UE.
6. UE chooses the prefered data to be shared and sends the user informaiton authorization response to IdP.
7. IdP send the authorized user information to SP.
8. After ueer data is sucessfully shared, RP sends a notification to UE.

editor's note: The datailed security mechanisms and technical details will be considered in next time.

5. Acknowledgements

The author would like to thank Klaas Wierenga, Hannes Tschofenig, Sam Hartman, Rhys Smith, Tao Fu, Zhengxue Xia for their valuable comments.

6. IANA Considerations

TODO

7. Security Considerations

TODO

8. References

8.1. Normative References

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[RFC4121] Zhu, L., Jaganathan, K., and S. Hartman, "The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API) Mechanism: Version 2", RFC 4121, July 2005.

[RFC4282] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", RFC 4282, December 2005.

[RFC4187] Arkko, J. and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", RFC 4187, January 2006.

8.2. Informative References

[I-D.ietf-abfab-arch]
Howlett, J., Hartman, S., Tschofenig, H., and E. Lear, "Application Bridging for Federated Access Beyond Web (ABFAB) Architecture", draft-ietf-abfab-arch-01 (work in progress), March 2012.

[I-D.ietf-abfab-usecases]
Smith, R., "Application Bridging for Federated Access Beyond web (ABFAB) Use Cases",

draft-ietf-abfab-usecases-02 (work in progress), February 2012.

[I-D.ietf-abfab-aaa-saml]
Howlett, J. and S. Hartman, "A RADIUS Attribute, Binding and Profiles for SAML", draft-ietf-abfab-aaa-saml-02 (work in progress), October 2011.

[I-D.jones-diameter-abfab]
Jones, M. and H. Tschofenig, "The Diameter 'Application Bridging for Federated Access Beyond Web (ABFAB)' Application", draft-jones-diameter-abfab-00 (work in progress), March 2011.

[I-D.ietf-abfab-gss-eap]
Hartman, S. and J. Howlett, "A GSS-API Mechanism for the Extensible Authentication Protocol", draft-ietf-abfab-gss-eap-05 (work in progress), March 2012.

[GSMA_IDM]
GSM Association, "White paper on Identity Management Requirements, Issues, and Directions for Mobile Industry", August 2007, <http://wiki.projectliberty.org/images/d/d8/GSMA_IDM_WP-SE47.pdf>.

[TelecoSiG]
Liberty Alliance Project, "Bridging IMS and Internet Identity", December 2009, <http://www.projectliberty.org/liberty/content/download/4315/28869/file/WP-BridgingIMS_AndInternetIdentity_V1.0.pdf>.

[TS33.220]
3GPP, "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)", 3GPP TS 33.220 10.0.0, October 2010.

[TR33.980]
3GPP, "Liberty Alliance and 3GPP security interworking; Interworking of Liberty Alliance Identity Federation Framework (ID-FF), Identity Web Services Framework (ID-WSF) and Generic Authentication Architecture (GAA)", 3GPP TR 33.980 10.0.0, April 2011.

[TR33.924]
3GPP, "Identity management and 3GPP security interworking; Identity management and Generic Authentication Architecture (GAA) interworking", 3GPP TR 33.924 10.1.0,

June 2011.

Author's Address

Yinxing Wei (editor)
ZTE Corporation
No 68, Zijinghua Road
Nanjing, Jiangsu 210012
China

Phone: +86 25 52872328
Email: wei.yinxing@zte.com.cn