CHANGE REQUEST

Title:	Addressing review comments on for ACR URI on IETF's uri-review mailing list	☒ Public ☐ OMA Confidential
To:	ARC REST-NetAPI	
Doc to Change:	OMA-TS-REST_NetAPI_ACR-V1_0-20140701-D	
Submission Date:	11 July 2014	
Classification:	☐ 0: New Functionality ☐ 1: Major Change ☒ 2: Bug Fix ☐ 3: Editorial	
Source:	Uwe Rauschenbach, Nokia, uwe.rauschenbach@nsn.com	
Replaces:	n/a	

1 Reason for Change

This CR changes Annex H which defines the ACR URI scheme to address review comments received on IETF's uri-review mailing list. Also, some leftovers from earlier versions of the text are fixed.

This CR will be kept in Postponed mode until the review at IETF is finished, and all needed updates have been collected.

2 Impact on Backward Compatibility

None

3 Impact on Other Specifications

None

4 Intellectual Property Rights

Members and their Affiliates (collectively, "Members") agree to use their reasonable endeavours to inform timely the Open Mobile Alliance of Essential IPR as they become aware that the Essential IPR is related to the prepared or published Specification. This obligation does not imply an obligation on Members to conduct IPR searches. This duty is contained in the Open Mobile Alliance application form to which each Member's attention is drawn. Members shall submit to the General Manager of Operations of OMA the IPR Statement and the IPR Licensing Declaration. These forms are available from OMA or online at the OMA website at www.openmobilealliance.org.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY THE OPEN MOBILE ALLIANCE OR ANY OPEN MOBILE ALLIANCE MEMBER OR ITS AFFILIATES REGARDING ANY OF THE IPR'S REPRESENTED ON THE "OMA IPR DECLARATIONS" LIST, INCLUDING, BUT NOT LIMITED TO THE ACCURACY, COMPLETENESS, VALIDITY OR RELEVANCE OF THE INFORMATION OR WHETHER OR NOT SUCH RIGHTS ARE ESSENTIAL OR NON-ESSENTIAL.

THE OPEN MOBILE ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS.

USE OF THIS DOCUMENT BY NON-OMA MEMBERS IS SUBJECT TO ALL OF THE TERMS AND CONDITIONS OF THE USE AGREEMENT (located at http://www.openmobilealliance.org/UseAgreement.html) AND IF YOU HAVE NOT AGREED TO THE TERMS OF THE USE AGREEMENT, YOU DO NOT HAVE THE RIGHT TO USE, COPY OR DISTRIBUTE THIS DOCUMENT.

THIS DOCUMENT IS PROVIDED ON AN "AS IS" "AS AVAILABLE" AND "WITH ALL FAULTS" BASIS.

5 Recommendation

ARC is requested to agree the CR.

© 2014 Open Mobile Alliance Ltd. All Rights Reserved.

Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.[OMA-Template-ChangeRequest-20110101-I]

6 Detailed Change Proposal

Change 1:

Appendix H. Definition of the acr: URI scheme (Normative)

This appendix is built on top of [RFC3966] and it specifies the URI (Uniform Resource Identifier) scheme "acr". This URI scheme is intended to be used in places where URIs following the ~~as an extension to the~~ "tel~~:~~" or "sip" scheme are normally used, but without disclosing the true identity of a reference or a user. The "acr" URI describes an anonymous reference that can be mapped to a resource or a user or a group of resources or users. There are multiple situations where the true identity of a user or a resource cannot be disclosed. The "acr" URI is an identifier ("name") only; it does not describe the steps necessary to reach the user or the device. However it can contain a parameter indication what body or organisation could resolve it. It is intended for privacy protection, where a user trusts a translating party that can route or forward the request or message to the ~~true~~ actual user or resource.

Informational note: This appendix is derived from the original proposal of the ACR concept [IETF ACR Draft] in the IETF. As it is closely related to the OMA RESTful Network APIs, this work was not pursued to completion in the IETF, but was transferred to and finalized in the Open Mobile Alliance.

H.1 "acr" URI syntax

The "acr" URI is defined using ABNF (Augmented Backus-Naur Form) as described in *[RFC5234]* and uses elements from the core definitions (appendix A of *[RFC5234]*).

~~The syntax definition follows *[RFC3986]*, indicating the actual characters contained in the URI. If t~~The reserved characters ~~"+",~~ ";"~~,"="~~, and "~~=?~~" are used as delimiters between components of the "~~tel~~acr" URI. ~~, t~~They MUST ~~NOT~~ be percent encoded, like other reserved characters, . ~~These characters MUST be percent encoded~~ if they appear in "~~tel~~acr" URI parameter values or as part of the anonymous-customer-identifier.

Characters other than those in the "reserved" and "unsafe" sets (see *[RFC3986]*) are equivalent to their "% HEX HEX" percent encoding.

The acr URI has the following syntax:

```
acr-uri                        = "acr:" anonymous-customer-reference
anonymous-customer-reference   = anonymous-customer-identifier *par
anonymous-customer-identifier  = 1*alphanum
par                            = parameter / network-code / acr-type / domainname
network-code                   = ";ncc=" 1*uric
acr-type                       = ";type=" 1*( "DYNA" / "STAT" )
domainname                     = ";domain=" *( domainlabel "." ) toplabel [ "." ]
domainlabel                    = alphanum / alphanum *( alphanum / "-" ) alphanum
toplabel                       = ALPHA / ALPHA *( alphanum / "-" ) alphanum
parameter                      = ";" pname [ "=" pvalue ]
pname                          = 1*( alphanum / "-" )
pvalue                         = 1*paramchar
paramchar                      = param-unreserved / unreserved / pct-encoded
unreserved                     = alphanum / mark
mark                           = "-" / "_" / "." / "!" / "~" / "*" / "'" / "(" / ")"
pct-encoded                    = "%" HEXDIG HEXDIG
param-unreserved               = "[" / "]" / "/" / ":" / "&" / "+" / "$"
alphanum                       = ALPHA / DIGIT
reserved                       = ";" / "/" / "?" / ":" / "@" / "&" / "=" / "+" / "$" / ","
uric                           = reserved / unreserved / pct-encoded
```

© 2014 Open Mobile Alliance Ltd. All Rights Reserved.

Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.[OMA-Template-ChangeRequest-20110101-I]

```
DIGIT                          = "0" / "1" / "2" / "3" / "4" / "5" / "6" / "7" / "8" / "9"
HEXDIG                         = DIGIT / "A" / "B" / "C" / "D" / "E" / "F" / "a" / "b" / "c" /
                                 "d" / "e" / "f"
ALPHA                          = lowalpha / upalpha
lowalpha                       = "a" / "b" / "c" / "d" / "e" / "f" / "g" / "h" / "i" / "j" /
                                 "k" / "l" / "m" / "n" / "o" / "p" / "q" / "r" / "s" / "t" /
                                 "u" / "v" / "w" / "x" / "y" / "z"
upalpha                        = "A" / "B" / "C" / "D" / "E" / "F" / "G" / "H" / "I" / "J" /
                                 "K" / "L" / "M" / "N" / "O" / "P" / "Q" / "R" / "S" / "T" /
                                 "U" / "V" / "W" / "X" / "Y" / "Z"
```

The "anonymous-customer-identifier" can be created from some suitable user or customer data such as phone number, and validation date. In order to provide anonymization, this data MUST not be included unchanged within the ACR. Rather it MUST be encrypted, hashed, represented by a look-up reference or otherwise obfuscated. The issuing provider is responsible for dereferencing the ACR to the user or resource. ~~For example the SHA-256 algorithm can hash the sensitive data:~~

~~SHA256("")= e3b0c442 98fc1c14 9afbf4c8 996fb924 27ae41e4 649b934c a495991b 7852b855~~

If it is required ~~In order~~ to know who issued the anonymous-customer-identifier, the network code (ncc) or domain name MUST be included, for cross-operator identification and to ensure it is known which entity can deference the ACR. ~~A URI for ACR documentation MAY be included; for example, to discover further meta-data, or to list the service endpoints which can consume the ACR.~~

The "network code" (ncc) for mobile networks is a concatenation of "mobile country code" (MCC) and "mobile network code" (MNC) as defined in [ITU-T E.212]. An example ncc of “23415” consists of the concatenation of MCC=“234” and MNC=“15”.

The “acr-type” indicates if the ACR is a static type or a dynamic type. An ACR of static type uniquely maps a persistent customer identifier (such as an MSISDN number) to an anonymous-customer-identifier value without expiry time, whereas an ACR of dynamic type allows reuse of the anonymous-customer-identifier value after a time period defined by service provider policies.

The anonymous-customer-identifier “auth” MUST NOT be assigned as an ACR to a particular user. It is reserved for use cases that determine the identity of the user by side information, such as an authorization token or particular network-based identification mechanisms, as specified in [REST_NetAPI_Common].

H.2 Examples (Informative)

acr:0123456890123456789

This URI points to a user. It is for network internal use only since the network code is not provided.

acr:0123456890123456789;ncc=12345

This URI points to a user belonging to the network with MCC=”123” and MNC=”45”.

acr:0123456890123456789;ncc=23415;type=DYNA

This temporal URI points to a user or group of users and can be resolved by the particular mobile network with MCC=”234” and MNC=”15”.

acr:0123456890123456789;ncc=123654

This URI points to a group of users belonging to the network with MCC=”123” and MNC=”654”. Note that the fact that more than one user is represented is not intrinsic to the ACR but only known to the issuing network.

acr:0123456890123456789;domain=example.com

This URI points to a user belonging in domain "example.com"

© 2014 Open Mobile Alliance Ltd. All Rights Reserved.

Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.[OMA-Template-ChangeRequest-20110101-I]

H.3 Rationale (Informative)

H.3.1 Privacy policies

Existing privacy policies and legislation restrict the sharing of certain user identifiers, such as the MSISDN, since it may be used to breach a user's privacy (unauthorized location look-up, cold calling, SMS Spam etc.). An ACR prevents such identifiers from being circulated.

H.3.2 Cookie support

Cookie support is inconsistent across mobile devices. An ACR can help identify a returning mobile user to a Website, and hence facilitate the provisioning of a personalized service based on previous preferences and activity.

H.3.3 Sharing identity

Mobile, broadband and other access networks do not typically share a user identifier. The ACR is not bound to a particular access network and can hence be used to provision user identifiers between networks.

H.3.4 Relation to SIP

The ACR can help the implementation of SIP privacy considerations, as detailed in [RFC3323], 'A Privacy Mechanism for the Session Initiation Protocol'. Specifically the ACR can be used as the value for the 'anonymous from' header field (see [RFC3323] section 4.1), and is consistent with the recommendation to remove Subject, Call-info, Organization, User Agent, Reply-To, In-Reply-To in [RFC3323] section 4.3.

H.4 Security Considerations

Since the ACR is used to protect the identity of a user or a device the forwarding party must not disclose information that would or can be used to reveal the identity of the user. However the network code or domain name will reveal some information of the user's affiliation or service provider.

The security considerations parallel those for the "tel" URI [RFC3966].

Web clients and similar tools MUST NOT use the "acr" URI to place telephone calls or send messages without the explicit consent of the user of that client. Placing calls or sending messages automatically without appropriate user confirmation may incur a number of risks, such as those described below:

- Calls or messages may incur costs.
- The URI may be used to place malicious or annoying calls.
- A call will take the user's phone line off-hook, thus preventing its use.
- A call may reveal the user's possibly unlisted phone number to the remote host in the caller identification data and may allow the attacker to correlate the user's phone number with other information, such as an e-mail or IP address.

This is particularly important for "acr" URIs embedded in HTML links, as a malicious party may hide the true nature of the URI in the link text, as in

```
<a href="acr:123456">Find free information here</a>
<a href="acr:123456">Call Foobar organization for help</a>
```

"acr" URIs may still reveal private information if the mapping from a user identity to an anonymous-customer-identifier is designed poorly. It is recommended to ensure that the anonymous-customer-identifier is sufficiently random, e.g. by applying a hashing step.~~, similar to including phone numbers as text. However, the presence of the "acr:" schema identifier may make it~~

© 2014 Open Mobile Alliance Ltd. All Rights Reserved.

Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.[OMA-Template-ChangeRequest-20110101-I]

~~easier for an adversary using a search engine to discover these numbers, and hence search engines should avoid indexing these identifiers.~~

It needs to be noted that hashing is prone to accelerated brute force attacks e.g. using rainbow tables; in particular if the space of clear text is small, as this may be the case if phone numbers are hashed directly. Countermeasures such as salting need to be considered. In addition, the use of a hash function that is strong enough (i.e. produces a sufficient number of bits) is required to prevent such attacks from being successful in practice.

H.5 IANA registration template

URI scheme name.
acr

Status.
provisional

URI scheme syntax.
See section H.1 in [1].

URI scheme semantics.
The "acr" URI describes an anonymous reference that can be mapped to a resource or a user or a group of resources or users, and that may include information which hints to an authority that can perform such mapping.

Encoding considerations.
The syntax definition above contains a complete enumeration of allowed characters, and contains provisions for percent-encoding of unsafe characters.

Applications/protocols that use this URI scheme name.
This URI scheme has been defined in [1] for use with a number of ~~the~~ OMA RESTful Network APIs (~~see~~ of which [2~~1~~] is an example).

Interoperability considerations.
This URI scheme has been defined for use with the OMA RESTful Network APIs. Multibyte character sets are not supported.

Security considerations.
See section H.4 in [1].

Contact.
Uwe[dot] Rauschenbach [at] nsn [dot] com

Author/Change controller.
OMNA - Open Mobile Naming Authority of the Open Mobile Alliance
OMA-OMNA [at] mail [dot] openmobilealliance [dot] org

References.

[1] OMA RESTful Network API for Anonymous Customer Reference Management, OMA-TS_REST_NetAPI_ACR-V1_0,_The Open Mobile Alliance. Published under http://technical.openmobilealliance.org/Technical/technical-information/release-program/current-releases/rest-netapi-acr-v1-0.

Open access to latest not-yet-published draft version at:
http://member.openmobilealliance.org/ftp/Public_documents/ARCH/Permanent_documents/OMA-TS-REST_NetAPI_ACR-V1_0-20140701-D.zip

Comment [UR1]: DSO – please do not put this part into the final specification

© 2014 Open Mobile Alliance Ltd. All Rights Reserved.

Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.[OMA-Template-ChangeRequest-20110101-I]

[2] OMA RESTful Network API for Chat, OMA-TS_REST_NetAPI_Chat-V1_0, The Open Mobile Alliance. Published under http://technical.openmobilealliance.org/Technical/technical-information/release-program/current-releases/restfulnetworkapi-chat-v1-0

Open access to latest not-yet-published draft version at: http://member.openmobilealliance.org/ftp/Public_documents/ARCH/Permanent_documents/OMA-TS-REST_NetAPI_Chat-V1_0-20140207-D.zip

Comment [UR2]: DSO – please do not put this part into the final specification

© 2014 Open Mobile Alliance Ltd. All Rights Reserved.

Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.[OMA-Template-ChangeRequest-20110101-I]