Network Working Group
Internet-Draft
Expires: Juanuary 12, 2006

M. Abid
INRIA
H. Afifi
Int
F. Kamoun
CRISTAL
N. Golmie
NIST

July 11, 2005

OSFR (Optimized network Selection for Fast Roaming)
draft-abid-eap-osfr-00

Status of this Memo

Copyright Notice

Abstract

In a public WLAN hotspot, we need to have an easy and secure way to authenticate users. We have to find also mobility solutions, given by providers, to perform well the roaming. A roaming mobile terminal MT may be within radio range of more than one access point AP. Therefore, we need to make an intelligent network selection decision after receiving some roaming information. Currently, the information is typically provisioned on the MTs as static roaming tables. But, this approach is not scalable when there is a large number of access points.

In this draft, we propose our solution called OSFR, Optimized Network Selection for Fast Roaming to improve association speed and scalability.

Table of Contents

1. Introduction

In a public WLAN hotspot, a roaming MT mobile terminal may be within radio range of more than one access point (AP). Therefore, we need to make an intelligent network selection decision after receiving some roaming information. Currently, the information is typically provisioned on the MTs as static roaming tables. But, this approach is not scalable when there are a large number of access points.

In this draft, we propose our solution called OSFR, Optimized Network Selection for Fast Roaming to improve association speed and scalability. It consists in piggybacking the information in the 802.11 Authentication Request/Response. The main advantage of our system is that we donÆt need to (re)associate each time with the new AP, rather associate only with the appropriate one which speeds up the connection procedure and results in a seamless handover.

1.1 Terminology

AAA

Authentication ,Authorization and Accounting

NAI

Network Address Identifier [rfc2486bis].

MT

Mobile Terminal

AP

The new Access Point that MT wants to associate with.

AAA Wlan Server

It is the Local Wireless LAN Server which has a list of vWISP virtual WISP that it has agreements with them.

AAA Mediating Server

The mediating Server that is localized in the path between AAA Wlan Server and AAA Home server.

AAA Home Server

The server which provides service for mobile node (MT has an account there).

For clarity, we will omit AAA from the terminology.

1.2 Applicability

Our solution is really helpful in these cases described in [ARK04]:

- o There is more than one available network attachment point, and the different points may have different characteristics.
- o The user has multiple sets of credentials. For instance, the user could have one set of credentials from a public service provider and another set from his company.
- o Providers share the same infrastructure, such as wireless access points.

The mobile terminal will need to associate with the right network, so that it can reach its home server. Especially, working in public places can causes high latency, especially, when the place is full of clients.

One of the problem that all people hate is the cut of receiving services. If we can not avoid it, at least, we try to reduce this time needed for network discovery and selection.

2. Design

One of the important characteristics of our solution is that we want to know the roaming information before getting associated with AP. We also need to send the information in a secure way because we work before the association and the channel isnÆt secure. Our idea is based on Diffie-Hellman Key exchange (D-H Key) [RFC2631] and optimized to use the 802.11 Management Frames [WIR03].

First of all, in Beacon frame, we add the two parameters needed to generate the D-H keys. Then, in Probe Request, MT sends its public key YMT and in Probe Response, AP sends its public key YAP. Now the two devices can send encrypted data with D-H keys. In IEEE 802.11 specification, we have two kinds of authentication algorithm (Open System and Shared Key). In our solution, using one of the two will not cause problems because we only use Auth Request and Auth Response for Open System, Auth Request and Challenge Text for Shared Key.

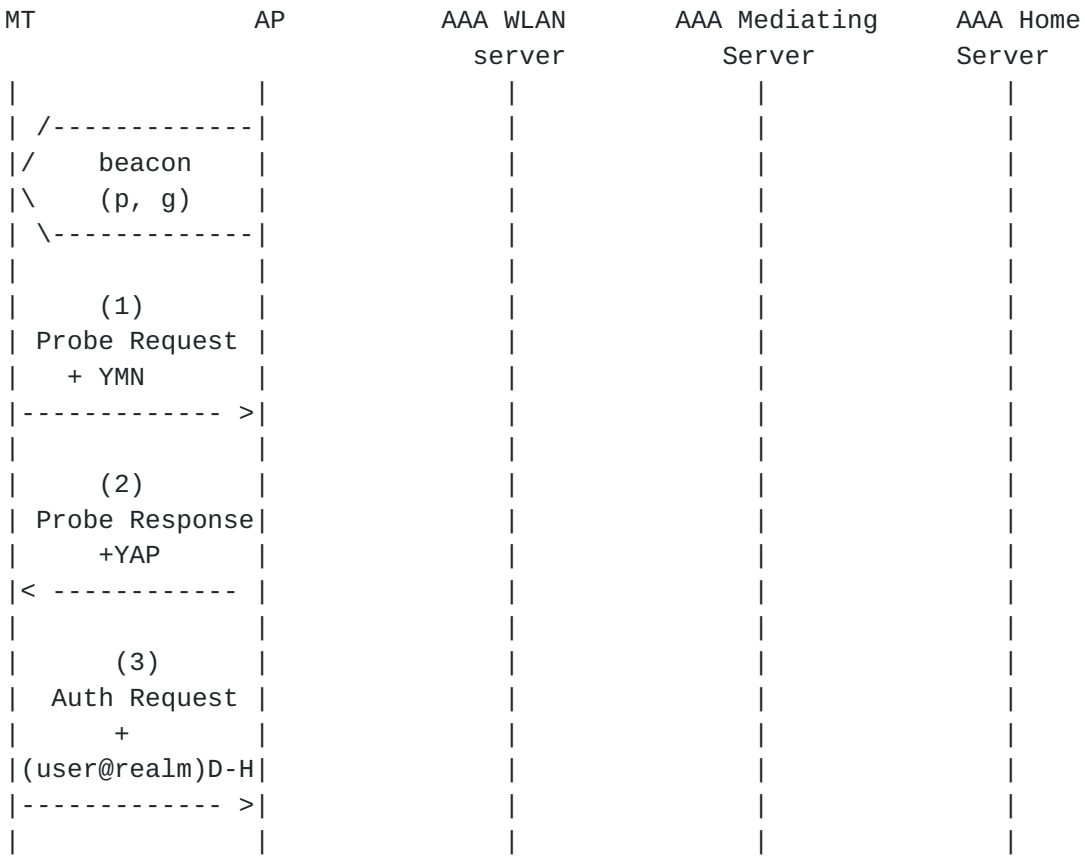
We aim to add roaming information which consists essentially in the identity of the intermediary WISP needed for Network Selection. If MT finds the WISP that it can reach its Home Server, it will send the identity of this Mediating Server. In that case, we will use the path passing by this Mediating Server in EAP session. We choose to send the list of WISP in the body of Management frame because this method helps us to use the maximum length for information.

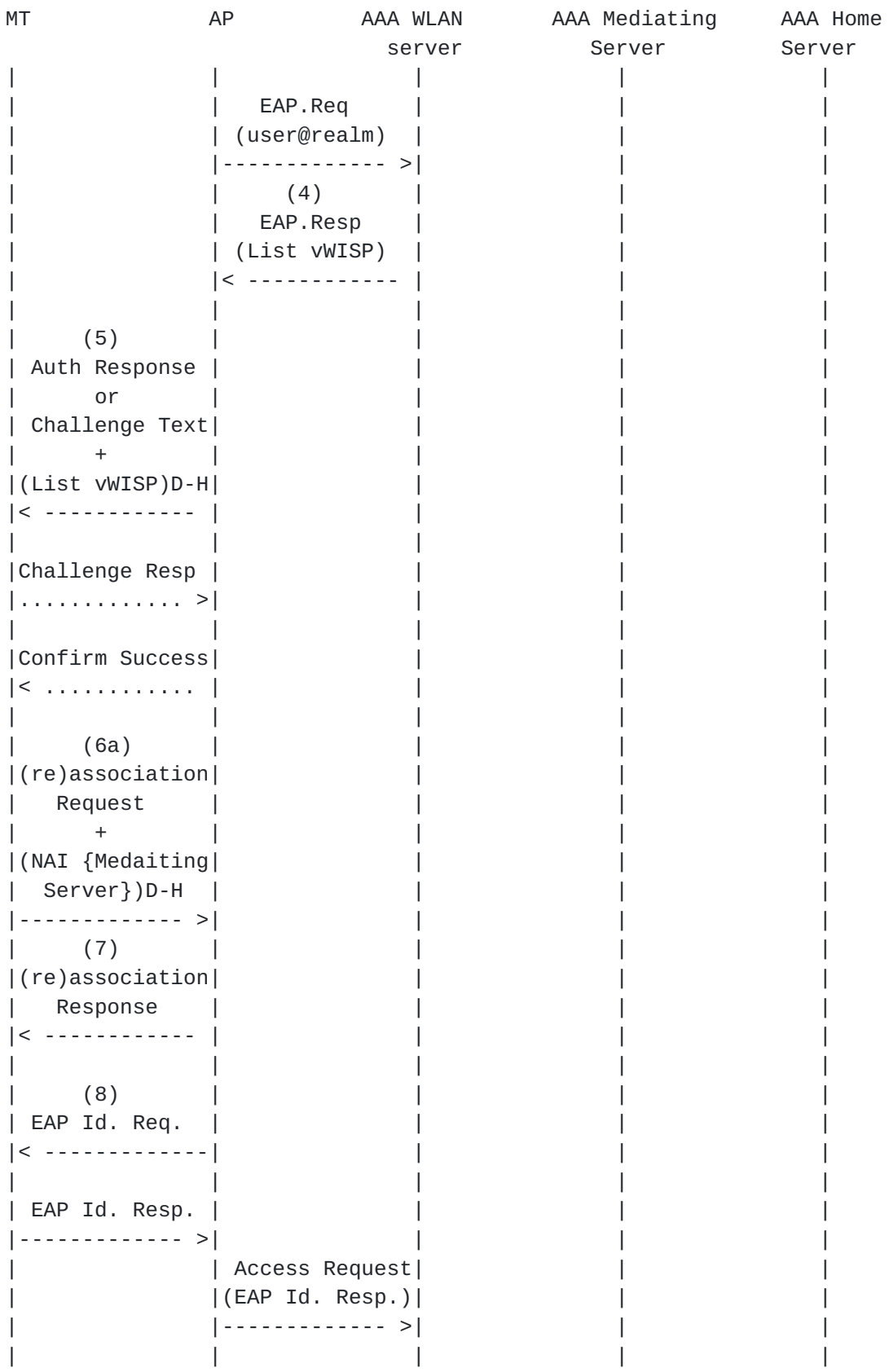
In some solution like Adrangi, et all [ADR05], the length used will be less than 1020 bytes. But when we use Management Frame body the least possibility will be when we piggyback information after Challenge Text and it will be 2048 bytes.

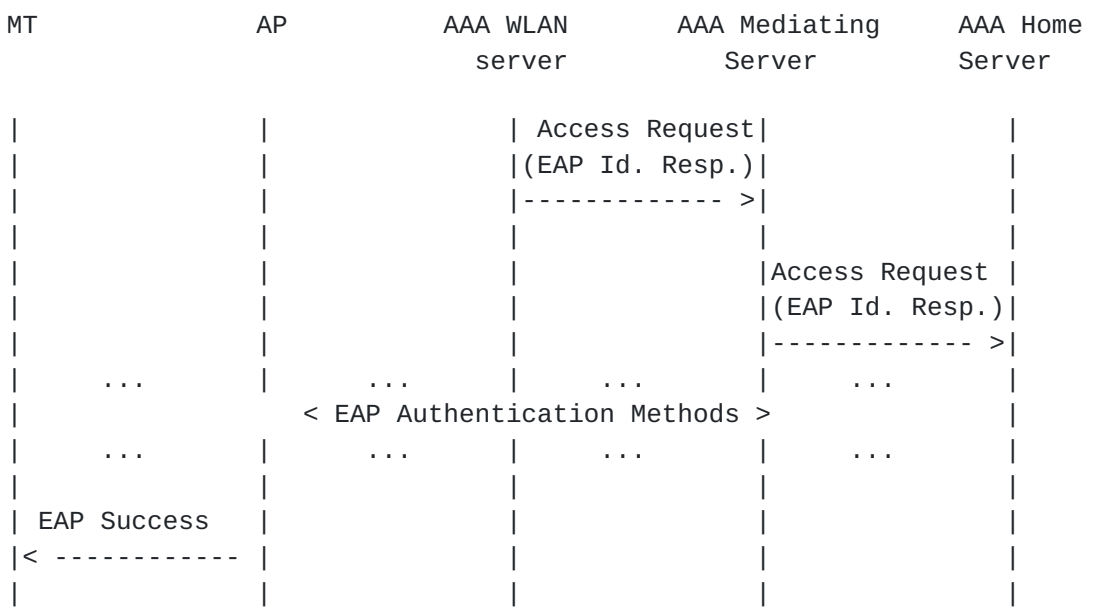
OSFR assumes also backward compatibility with devices that do not support this technique. LetÆs give now more details about how OSFR performs.

3. Scenario

In this scenario, we present all possible interactions between the actors. In the fellowing, we see all the message in OSFR scenario.




MT
AP
AAA WLAN server
AAA Mediating Server
AAA Home Server
EAP.Req (user@realm)
(4)
EAP.Resp (List vWISP)
(5) Auth Response or Challenge Text + (List vWISP)D-H
Challenge Resp
Confirm Success
(6a) (re)association Request + (NAI {Medaiting Server})D-H
(7) (re)association Response
(8) EAP Id. Req.
EAP Id. Resp.
Access Request (EAP Id. Resp.)



AP sends Beacon to alert the users about its presence. In our solution, AP is the one who chooses the parameters (prime number 'p' and base 'g') needed to generate the D-H keys. Here are all possible interactions in our scenario:

1 When MT sends to AP a Probe Request, it piggybacks its public key YMT.

2 AP sends Probe Response to MT and piggybacks its public key YAP. After exchanging the public keys, we can begin a secure session using D-H keys. Our modification will not depend on the type of IEEE 802.11 Authentication.

3 MT sends an Authentication Request including its identity user@realm encrypted with D-H key.

4 AP will send the identity in an EAP Request to WLAN Server. This later has a list of vWISP virtual WISP. WLAN Server will send the list to AP within an EAP Response.

5 A can be the Authentication Response "Open System" or the Challenge Text "Shared Key". AP piggybacks the list (encrypted with D-H key). MT needs this list to choose the "right" Mediating Server to reach its Home Server. If we choose Open System, we pass directly to (re)association. Otherwise, if it is Shared Key, we continue to send the Challenge Response and Success Access.

6 Now, all depends on the list received by MT:

6a MT doesnÆt find the right Mediating Server in the list sent by AP; it will not (re)associate with AP and will seek for another one. For example, MT wants a French WISP but in the list there is only American WISP.

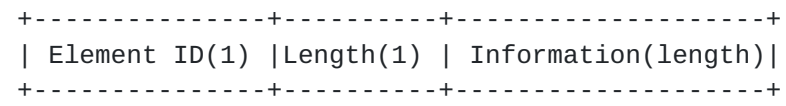
6b In the other case, MT sends (re)Association Request and piggybacks the NAI of the Mediating Server encrypted with D-H key.

7 AP sends (re)Association response to MT.

8 Now, EAP session can begin and we are sure that WLAN Server will reach the Home Server using a path including the chosen Mediating Server.

4. Packet Format

In this section, we introduce all the changes that we need to do in the body of some Management Frames. The maximum size of the frame body is 2312 bytes. We will add some new Information Elements that have 3 fields:

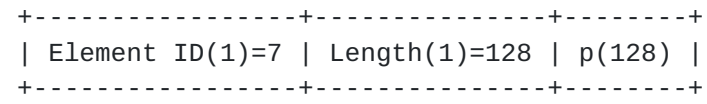


We found in the IEEE 802.11 specification some reserved element ID (7-15, 32-255). We project to use some of this element ID to add our new Information Elements. The length given between () is in bytes for all fields.

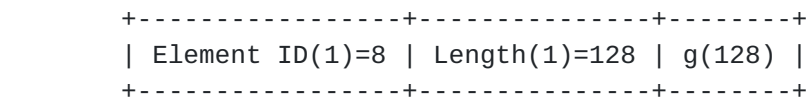
4.1 Beacon

We piggyback the prime 'p' and base 'g'. The length of the parameters 'p' and 'g' will be 1024 bits (128 bytes). In the IEEE 802.11 specification, the maximum length free in Beacon frame body is 334 bytes. We just add after TIM (Traffic Indication Map) 2 new fields one for parameter 'p' and the other for 'g'. The length of each field is 128 bytes.

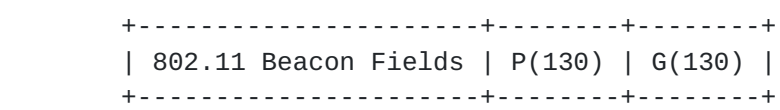
P: Information Elements



G: Information Elements

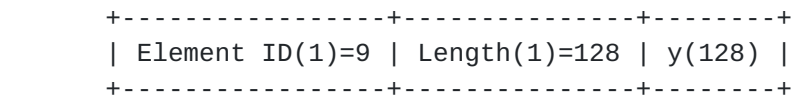


The new beacon frame body seems like:



4.2 Probe Request

In the probe request, we add the MTÆs public key YMT. The later will be a new element information.



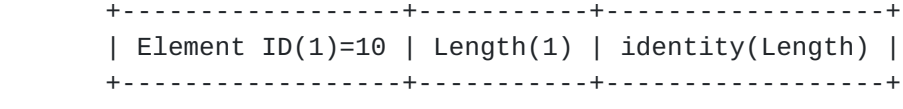
The new Probe Request frame body seems like:

4.3 Probe Response

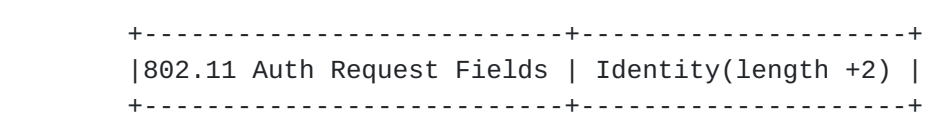
It is like Probe Request but source now is AP. We have the same Information Element y (Element ID=9) called YAP. The new Probe Request frame body seems like:

4.4 Authentication Request

Identity is a string which identifies user (ex mail address, login). The new Element Information contains the identity encrypted by D-H key. The max length of Identity will be 2304 bytes.

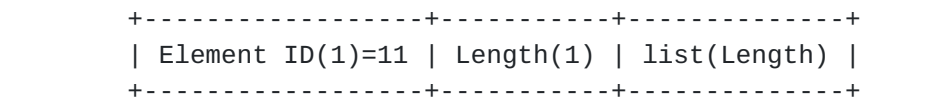


The frame body will be:

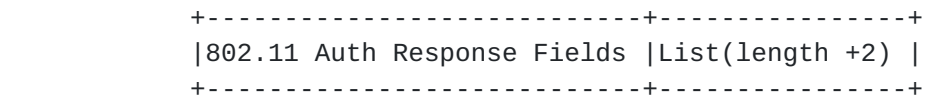


4.5 Authentication Response or Challenge Text

We add a new Element Information called List (encrypted with D-H key).

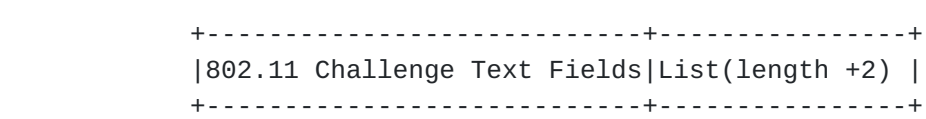


1 If Authentication algorithm number equals 0 (Open System), the frame body will be:



Here the maximum length of List is 2304 bytes.

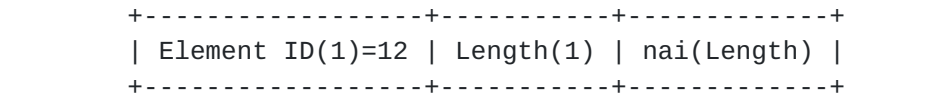
2 If Authentication algorithm number equals 1 (Shared Key), the frame body will be:



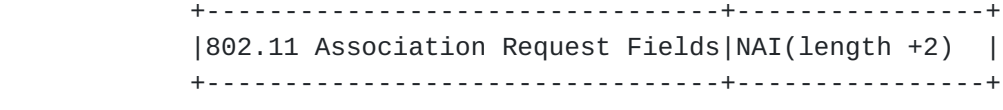
Here the maximum length of List is 2048 bytes. The 2 next frames in Shared Key Authentication wonÆt be modified.

4.6 (Re)Association Request

Here we will add the last new Information Element NAI. It is the identifier of the Mediating Server (encrypted with D-H key). The maximum possible length for NAI is 2262 bytes.



1 If we have Association Request, the frame body will be:



2 If we have Re-association Request, the frame body will be:

The final (re)Association response will not be changed.

5. Security Considerations

OSFR use Diffie Hellman to secure the exchange of encryted data in the management level. All the security in this system is provided by the secrecy of the private keying material. If either sender or recipient private keys are disclosed, all messages sent or received using that key are compromised. Similarly, loss of the private key results in an inability to read messages sent using that key [RFC 2631].

6. Acknowledgments

The authors would like to thank Walid Dabbous and our colleagues at Planete team for their comments and suggestions. Also, we thank the members of CRISTAL Laboratory.

References

[ARK04] J. Arkko and B. Aboba, "Network Discovery and Selection Problem", draft-ietf-eap-netsel-problem-02, October 2004.

[WIR03] ANSI/IEEE Std 802.11, 1999 Edition (R2003), Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[ADR05] F. Adrangi, V. Lortz, F. Bari, P. Eronen. "Identity selection hints for Extensible Authentication Protocol (EAP)", draft-adrangi-eap-network-discovery-and-selection-13.txt, May 2005.

[RFC2631] E. Rescorla, "Diffie-Hellman Key Agreement Method", RFC 2631,June 1999.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[rfc2486bis] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", draft-ietf-radext-rfc2486bis-05 (work in progress), July 2004.

Authors' Addresses

Mohamed Abid
INRIA Sophia Antipolis
2004 route des lucioles
BP 93 06902 Sophia Antipolis
France

EMail: Mohamed.Abid@sophia.inria.fr

Hossam Afifi
INT
9 rue, Charles Fourier
Evry 91011
FRANCE

Phone: +33 1 60 76 47 08
EMail: Hossam.Afifi@int-evry.fr

Farouk Kamoun
CRISTAL ENSI
Universit de la Manouba
2010
Tunisia

Phone: +216 71 600 444 / +216 98 328 083
EMail: Farouk.kamoun@ensi.rnu.tn

Nada Golmie
NIST
100 Bureau Drive, Mail Stop 8920,
Gaithersburg, Maryland, U.S.A.
Phone: +1 301-975-4190
Mail: nada.golmie@nist.gov

Intellectual Property Statement

Full Copyright Statement

Disclaimer of Validity