International Roaming Access Protocols (IRAP) Framework

Intel Corporation
Corporate Technology Group

1 December 2004
Agenda

- Objectives and Overview
- Need for Roaming Interfaces
- Roaming Architecture
- Next Steps
Roaming Vision

Network Access
- Personal Profiles & Preferences
- Public WLAN Hotspots
- 2.5G / 3.0G Networks
- Enterprise LAN / WLAN Networks
- Residential WLAN

Device Access

Services Access
- Voice Services
- Commerce
- Fleet Mgmt
- CRM
- Video Svcs
- VPN
- Location Info
- E-Mail
- SMS & MMS
- Internet

* Third party brands/names are property of their respective owners
Achieving "Seamless Roaming"

- Consistent sign-on for different wireless networks
- Mutual authentication using multiple wireless devices
- Multi-credential support within & across roaming alliances
- Security consistent with Enterprise WLAN policies
- Consolidated bill for wireless usage

Mutual authentication using multiple wireless devices

Consistent sign-on for different wireless networks

Multi-credential support within & across roaming alliances

Security consistent with Enterprise WLAN policies

Consolidated bill for wireless usage
Serve Your Customers Anywhere

Access Network Association

Operator owned Access Network

Local Hotspot / Access Network

Internet

Home Service Provider

Network Access Authorization

* Third party brands/names are property of their respective owners
New Service Opportunities

- Bring Internet growth to wireless services

![Universal IP Connectivity](image)
All IP Svcs Require IP Connection

Steps 3, 4, 5, ...

NGN svcs: Voice, IMS (3GPP, TISPAN, ITU, etc.)

UMA or SIP voice

3GPP R7

IPSEC, VPN, etc.

Step 2

Enhanced service authorization & provisioning

Step 1

Universal IP Connectivity

Client

Association

Access network

Roaming Agmt

Svc Provider

Services support Discovery

* Third party brands/names are property of their respective owners
No IP Connection ➔ No IP Svcs

Steps 3, 4, 5, …

1. Universal IP Connectivity
   - Services support Discovery

2. Service discovery, authorization & provisioning
   - NGN svcs: Voice, IMS (3GPP, TISPAN, ITU, etc.)
   - UMA or SIP voice
   - 3GPP R7
   - IPSEC, VPN, etc.

Client Association Access network Roaming Agmt Svc Provider
Bringing Internet Growth to Wireless

• Make it safer:
  • add a greater level of security to authentication

• Make it simpler:
  • move from manual to automated connections

• Make it seamless:
  • interwork with other hotspots and networks
The issue at hand

- Fragmentation in the PWLAN ecosystem
  - Rapid deployment of PWLAN hotspots and equipment
  - Variety of deployment strategies could result in fragmented and incompatible implementations
    - Many choices exist within the standards
  - Increases the cost and complexity of supporting global PWLAN roaming between operators

Need to enable safer, simpler, standards-based methods of network access
WLAN Standards and Forums

Standards

Protocols

ITU
IEEE: Wireless, Security, QoS foundation

IETF: common AAA protocols

Domain Solutions

3GPP2

3GPP: Promoting use of IETF, IEEE standards

 Forums

GSMA: consistent usage and deployment models

Wi-Fi Alliance: Overall Wi-Fi focus, client – AP interaction

IPDR: settlement format for billing exchange

Interop

Testing

IRAP

© 2004 Intel Corporation

* Third party brands/names are property of their respective owners
Universal IP Connectivity Goals

• Define common interoperable interfaces or profiles between network entities
• Reduce fragmentation by early alignment with existing and emerging standards
• Facilitate operator / vendor adoption of the interfaces
• Better security and roaming enables more advanced services
• Scope: AAA interworking for Universal IP Connectivity
Agenda

- Objectives and Overview
- Need for Roaming Interfaces
- Roaming Architecture
- Next Steps
**Trust Model for WLAN**

- Mobile Client doesn’t trust Foreign WLAN to provide safe service
- Foreign WLAN doesn’t trust Mobile Client to pay its bill

- Mobile Client trusts Home WLAN to provide safe service
- Home WLAN trusts the Mobile Client to pay its bill

- Foreign WLAN and Home WLAN trust each other to pay Mobile Client charges
- Foreign WLAN and Home WLAN trust each other to bill only for legitimate activity

Third party brands/names are property of their respective owners
## Cellular ≠ Wi-Fi

<table>
<thead>
<tr>
<th>Comparison</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>You will be prosecuted if you operate an unlicensed transmitter in a cellular band</td>
<td>Anyone can legally deploy a Wi-Fi access point (unlicensed band)</td>
</tr>
<tr>
<td>Erecting and operating a cellular tower costs significant $$$s</td>
<td>You can deploy and operate a Wi-Fi access point for $&lt; 100</td>
</tr>
<tr>
<td>Cellular base stations and towers occupy fixed locations</td>
<td>A rouge AP is transportable anywhere</td>
</tr>
<tr>
<td>The cellular operator owns all the equipment, in physically secure sites</td>
<td>Wi-Fi equipment is owned by a mix of carriers, hot spot providers, enterprises, and individuals in sites with varying security levels</td>
</tr>
<tr>
<td>There are only a small number of Cellular operators world-wide</td>
<td>The number of access point operators is legion</td>
</tr>
<tr>
<td>Session keys can only be used within the cellular network itself, where their use can be audited</td>
<td>Session keys can be transported to (rogue) APs that are not auditable</td>
</tr>
<tr>
<td>Except for special cases, the only thing worth stealing in a cellular network is service, and there are easier ways to accomplish this than cryptanalysis</td>
<td>The IPR on computer hard drives is more valuable than the WLAN communication itself</td>
</tr>
</tbody>
</table>
Need for standard interfaces

Clients → Access Network → Home operators → Billing/Clearing

1. Network Access
2. Authentication & Authorization
3. Accounting Data

* Third party brands/names are property of their respective owners
Interoperable Interfaces

- Interface definition: specification of a set of protocols and associated behavior through which two components of a network system interact

- Well-designed interfaces foster both interoperation and innovation
  - Interfaces should be designed with end-to-end system operation in mind
  - Innovation occurs within components and subsystems

- Interface requirements
  - Standards-based
  - Concrete and testable for conformance verification
  - Coexistence with legacy solutions, provide migration path
Agenda

• Objectives and Overview
• Need for Roaming Interfaces
• Roaming Architecture
• Next Steps
Architectural Tenets

- **Usability**
  - Common login process
  - Simplified client provisioning
  - Seamless roaming experience

- **Security**
  - Mutual authentication to protect user & network
  - Multiple client credential types, e.g. password, SIM, certificates
  - Secure tunnels for back-end authentication
  - Support VPN for remote enterprise access

- **Scalability / Extensibility**
  - Accommodate various wireless topologies
  - Ability to share infrastructure safely
  - Support advanced services efficiently
  - Common accounting data
Roaming Architecture & Protocols

Access Network (hot spot)

Home Network

RADIUS AAA Server / gateway

Wireless Station

Access Controller

RADIUS AAA

EAP Methods (e.g. EAP-SIM, EAP-MSCHAPv2, …)

PEAP / TTLS

WPA Authentication & over-the-air Encryption

802.1X / PKM2

802.11 / 802.16e

802.3 / IP

Provisioning and Authentication over PEAP or TTLS

Intel Research & Development

* Third party brands/names are property of their respective owners
IRAP Roaming Interfaces

- Develop industry-standard Interface Profiles
  1. Wireless Station to Access Network – Roaming user login
  2. Access Network to Home Service Provider authentication system
     – Roaming user authentication
  3. Access Network to billing system
     – Session accounting for One Bill Roaming
  4. Access Network to Home Service Provider operations subsystem
     – services support discovery & customer support services

IRAP = International Roaming Access Protocols

* Third party brands/names are property of their respective owners
Agenda

- Objectives and Overview
- Need for Roaming Interfaces
- Roaming Architecture
- Next Steps
IRAP Program Outline

- Use existing standards
  - Industry feedback: “We have enough WLAN standards. Don’t define more, make the ones we have work.”
- End to end solution
  - Unique aspect is the end to end approach – crosses multiple standards bodies and unifies the otherwise fragmented landscape.
Deployment

• Completed Trials in Singapore
• Industry influence
  • Wi-Fi Alliance, IETF RADEXT and GEOPriv WGs, GSMA IREG, ETSI TISPAN
• Current Forum Members and Participants
  • AntLabs
  • HuaWei
  • SingTel
  • TeliaSonera
  • Cetecom
  • iPass
  • SwissCom
  • Telia HomeRun
  • Cisco
  • Microsoft
  • EuroSpot
  • Telus Mobility
  • DanNet
  • RoamPoint
  • SwissCom Mobile
  • TheCloud

* Third party brands/names are property of their respective owners
Summary

• Industry needs global WLAN interoperability specs & testing methodologies

• IRAP program goals:
  • Well-defined architectural blueprint for PWLANs, allows for migration to safer, simpler authentication
  • A standards-based set of interfaces to facilitate global roaming and interoperability
  • A complete validation package

• Now is the time to engage in IRAP
For more information

- Documentation and Information on Intel roaming programs
  - [http://www.intel.com/technology/roaming](http://www.intel.com/technology/roaming)

- Direct link to IRAP documentation and information
  - [http://www.intel.com/go/irap](http://www.intel.com/go/irap)

- Direct link to Wireless LAN End to End Guidelines

- For more information on Intel R&D
  - [http://www.intel.com/technology](http://www.intel.com/technology)
Backup
Intel Quickens Race To Expand Range Of Wireless World

... the chip maker said five Asian telecommunications companies were joining its collaboration ... China Mobile Ltd. in China; MobileOne Ltd., Singapore Telecommunications Ltd. and StarHub Pte. Ltd. in Singapore; and PCCW Ltd. in Hong Kong.

The Asian Wall Street Journal, 16 September 2003

* Other names and brands may be claimed as the property of others.
IRAP

- IRAP = International Roaming Access Protocols
- IRAP = Technology Package (framework)
  - Common Interface profiles defines interoperability
  - Validation Plan confirms interoperable implementation
  - Built on Intel/IDA test bed results
- IRAP = Industry Program
  - Develop industry test/validation ecosystem
  - Promote adoption and deployment of IRAP framework

* Third party brands/names are property of their respective owners
Intel Contributions: Roaming Specifications

- Industry standards work
  - IEEE – .11e chair, .11i editor, 802.21 editor, …
  - IETF – AAA, EAP
  - 3GPP – SA2, SA3, CN4
  - 3GPP2 – WLAN Interworking
  - ETSI – TISPAN

- Industry Forum work
  - GSMA – WLAN Task Group, e-Commerce, …
  - WiFi Alliance – board member, Ease of Use chair, Public Access editor, etc.
Interface 1 Scenario

Interface between the client and the access network

- Technical support for:
  - Co-existence of UAM and 802.1X/WPA
  - Multiple credential types
  - Access Control
  - Intermediary network discovery and selection
  - NAI decoration
  - Draws on WiFi Alliance, IETF, and IEEE

© 2004 Intel Corporation
* Third party brands/names are property of their respective owners
Interface 2 Scenario

Interface between the access network and the home operator’s authentication & authorization system

• Technical support for:
  • Mutual authentication of client and network
  • RADIUS attribute handling
  • Intermediaries, RADIUS AAA routing
  • Early Termination
  • AP-AC considerations
  • GSMA IR61 and IETF RADIUS EXT

* Third party brands/names are property of their respective owners
Interface 3 Scenario

Interface between the access network and the home operator’s accounting system

- Technical support for:
  - Complete set of accounting data required to support multiple charging models for billing.
  - Scalability – where data clearinghouses are used
  - Location, Billable Identity attributes in accounting records
  - GSMA IR61 and IETF RADIUS EXT
Interface 4 Scenario

Interface between the access network and the home operator’s customer support system

- Technical support for:
  - Secure access to site status information
    - Push, pull, and event-driver models
  - Information on customer login process
  - Protocol used between visited hotspot and home network
    - Security, reliability, overhead, extensibility
IRAP development

- **Step one: Spec/tests defined with informal working group (v 0.1 – v1.0)**
  - Broad industry consensus
  - Includes parties important in deployment, but without formal industry participation
  - Focus is on getting rapid initial alignment

- **Step two: Transition to formal, industry recognized process – this is where ETSI is attractive.**
  - Expect to standardize both interfaces and conformance tests for interfaces

- **Status:**
  - Interface spec is 0.89
  - Conformance is 0.5
802.1X Overview

- STA 802.1X blocks port for data traffic
- AP 802.1X blocks port for data traffic
- 802.1X/EAP-Request Identity
- 802.1X/EAP-Response Identity (EAP type specific)
- EAP type specific mutual authentication
- Derive Pairwise Master Key (PMK)
- 802.1X/EAP-SUCCESS
- RADIUS Access Request/Identity
- RADIUS Accept (with PMK)
- Derive Pairwise Master Key (PMK)
- RADIUS Access Request/Identity
- RADIUS
Need for WLAN Security

• Expect enterprise users to drive most of the early revenues for public WLAN usage
  • Improved security solutions will impact deployment decision for 90% of executives**

• User concerns
  • Authentication
    • Can user credentials be stolen?
  • Data privacy
    • Can wireless traffic be decrypted?
    • Can data be intercepted?
  • Network “goodness”
    • Are users connected to valid networks?

** Source: Jupiter Research, executive surveys, 2003

* Third party brands/names are property of their respective owners
Public Access and VPNs

• Ability to secure traffic with a VPN connection is “necessary but not sufficient”
  • VPNs do not secure the authentication process
  • Users may not want to connect back to the corporate network
  • Users may still connect to the internet if the VPN server happens to be unreachable