



# COA<sup>1</sup> Paper

## Secure Protocols – Mobile Management

This paper augments the Jericho Forum<sup>®</sup> COA Technology paper “Secure Protocols - Wireless” highlighting the practical problems in the operation of wireless networks to be solved as de-perimeterisation delivers the security architecture to roam effectively.

### Problem

For a truly mobile device, operating to de-perimeterised principles, a wireless connection is probably required to achieve optimal connectivity while roaming. From a security stance, all foreign networks, wired or wireless, should be regarded as hostile. However the ability to make a transparent wireless connection remains elusive due to the lack of standards in this area (especially around Wi-Fi) that inhibits the exploitation of de-perimeterisation.

### Why should I care

The use of mobile devices and applications designed to the Jericho Forum blueprint implies that mobile working should be a seamless user experience.

Adopting de-perimeterised principles, where the end device is assumed to be in a hostile environment (whether on an internal or public IP address) and security designed appropriately, is ideal for working in the wireless world.

However, the issue of working in a foreign (or public) networked environment, whether wired or wireless, is the inability to control the network experience of the user, from Quality of Service (QoS), connection authentication or cost of the connection thus negating many of the advantages to the user of a de-perimeterised solution.

### Challenges to the industry

#### In a corporate environment

In both a wired and wireless corporate environment the primary problem to be solved is whether the device is permitted to connect to the network, and consume both network and corporate resources; primarily bandwidth, both Intranet and Internet.

In an environment where corporate devices are connecting to a corporately managed network, access authorisation solutions can be performed using 802.1x or other such access mechanism. Integrating this with RADIUS and corporate directory services will ensure that the connection is transparent to permitted users or devices.

Identity federation has the potential to allow devices from business partners and other trusted users also to authenticate – identifying those users as “trusted” means they could potentially be subject to different bandwidth and QoS rules.

---

<sup>1</sup> The Collaboration Oriented Architectures (COA) paper and COA Framework paper are both available at <http://www.opengroup.org/jericho/publications.htm>

For devices unable to authenticate (probably guests/visitors) the connection will depend on corporate policy with the device possibly being allowed to connect subject to an interactive user login. While transparent Internet access via a wired connection is feasible, many companies will be reluctant to extend the same openness via a wireless network for fear of uncontrolled abuse by the non-visitor.

### **In an external corporate environment**

In an external corporate environment the issue is as above but reversed. It will depend on what facilities they have in place to manage guest or visitor connectivity. In an enlightened world they will also be de-perimeterised and thus allow connections using their network.

### **In a public environment**

Once outside the managed corporate environment the problems begin with variable standards to manage connection. In the Wi-Fi domain, there is the promise of a fast and simple connection with performance equivalent to a wired connection. However, with no standard for authentication and charging, most users connecting to public Wi-Fi attempt but rarely complete the connection. With no public “cell-handover” use while mobile in this environment is almost always doomed to failure and thus restricted to “static” use in hotels (generally as a wired alternative).

In the cellular world, the connections are generally slower but access is more transparent to the user. However, high data charges and extortionate roaming charges make this restrictive for many; use while on the move usually works well and is reliable.

### **Issues when outside the corporate environment**

- Authentication to a foreign network is rarely transparent
- The cost of the connection varies with the medium used and the location
- There is a diverse set of charging and payment / collection mechanisms
- A least-cost / highest-bandwidth connection cannot be automated (scripted) with an increasing number of options available (Wired, WiFi, WiMax, GPRS, 3G).
- No standard method exists for understanding cost and bandwidth for making connection options based on corporate policy (and the ability to express that policy electronically)

There are companies who specialise in aggregating various forms of remote connectivity and, when working in a part of the world where that “club” has agreements in place, reasonably seamless connectivity can be achieved. However this is neither true roaming nor true de-perimeterisation. Where applications are reliant on session integrity (e.g. voice) then the application needs to design out, if possible, the effect of a variable quality connection that mobile usage delivers.

### **Assumptions**

When connecting via wireless then the security of the data should not be reliant on the network, as the transport mechanism will provide no integrity for the data and the confidentiality and integrity aspects of security will be provided by inherently secure protocols (JFC#4<sup>2</sup>) or secured data (JFC#11).

Inspection and understanding of the protocol in use (while not of the data itself) will allow traffic type to be determined and thus allow QoS to be applied where feasible. The origin and destination of data packets can be inferred while operating in any network environment.

---

<sup>2</sup> The term JFC#n refers to the relevant Jericho Forum Commandment number. See [www.jerichoforum.org](http://www.jerichoforum.org)

## The way forward

Key to making transparent mobile de-perimeterised working a reality is the ability to express the Wi-Fi hotspot “contract” (rate & other costs) electronically . The client must also transparently try to authenticate the network itself (JFC#7), understanding http/https redirected login pages and 802.1x, such that an automatic decision can be made to allow (or deny) a connection based on corporate or personal policies.