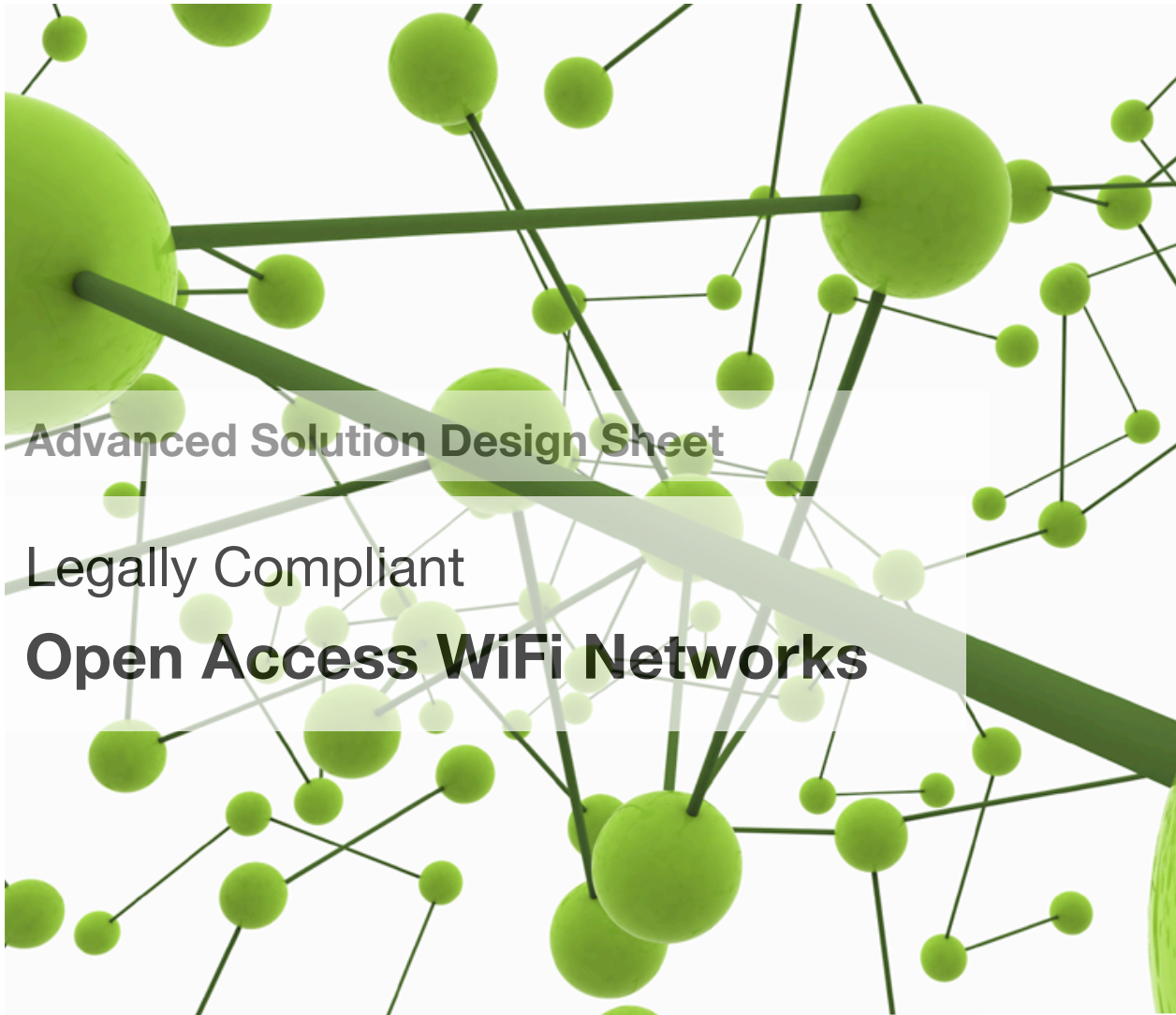




axiros
Lasting Advantage



axess
Device Management



Advanced Solution Design Sheet

Legally Compliant

Open Access WiFi Networks

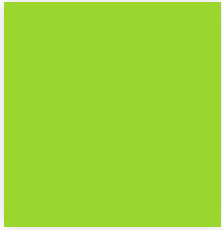
Axiros GmbH

Germany
Rosenheimer Str 30-32
81669 Munich

T +49 89 54 99 89 700
F +49 89 67 97 17 07
www.axiros.com
info@axiros.com

Open Access WiFi Networks

Fully Enabled for Data Retention and Lawful Intercept



Introduction

Data Retention and Lawful Intercept at Internet Service Providers

introduction

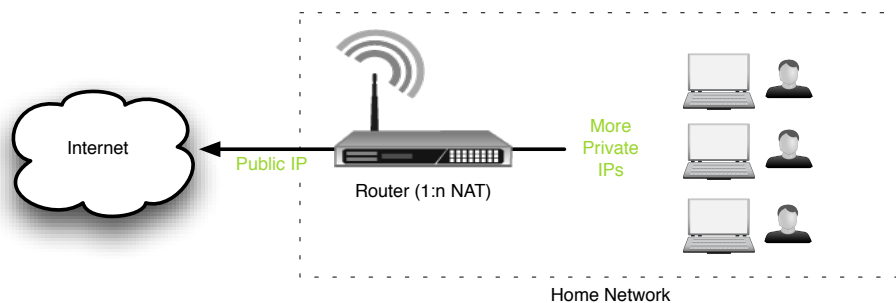
In recent years legal standards regarding Lawful Intercept and Data Retention have become binding for Internet Service Providers and Mobile Network Operators. In the paper we illustrate an architecture which can fulfill these requirements also in large managed wireless access networks, with their specific challenges in a robust and highly scalable way, using only slight modification to best of breed Common of the Shelf standard technologies.

Lawful Intercept, Li, is the process of intercepting within a network, communications between parties of interest to Law Enforcement Agencies. The interception is legally authorised and is conducted without the intercepted parties being aware of it. Law Enforcement Agencies include state and federal police, intelligence agencies and independent commissions against corruption. Lawful Intercept is often referred to as 'wiretapping' or 'phone-tapping'.

Data Retention, DR (or data preservation) generally refers to the storage of call detail records (CDRs) of telephony and Internet traffic and transaction data by governments and commercial organisations. In the case of government data retention, the data that is stored is usually of telephone calls made and received, emails sent and received and web sites visited. Further, location data is also to be collected.

Within this paper we deal exclusively with handling requirements for Internet Service Providers (ISPs) and not (mobile) telephony.

ISPs have invested significantly in building up infrastructures which comply with DR and LI requirements in their core business - providing Internet access for their subscribers withing their homes or (small) offices. These are small area networks with a restricted number of users, (personally) well known to the subscriber. Their traffic in the Internet is sourced from the one current public address the subscriber got from the ISPs and which is translated typically by a consumer router from within a home network of private IPs.



Axiros GmbH

Germany
Rosenheimer Str 30-32
81669 Munich

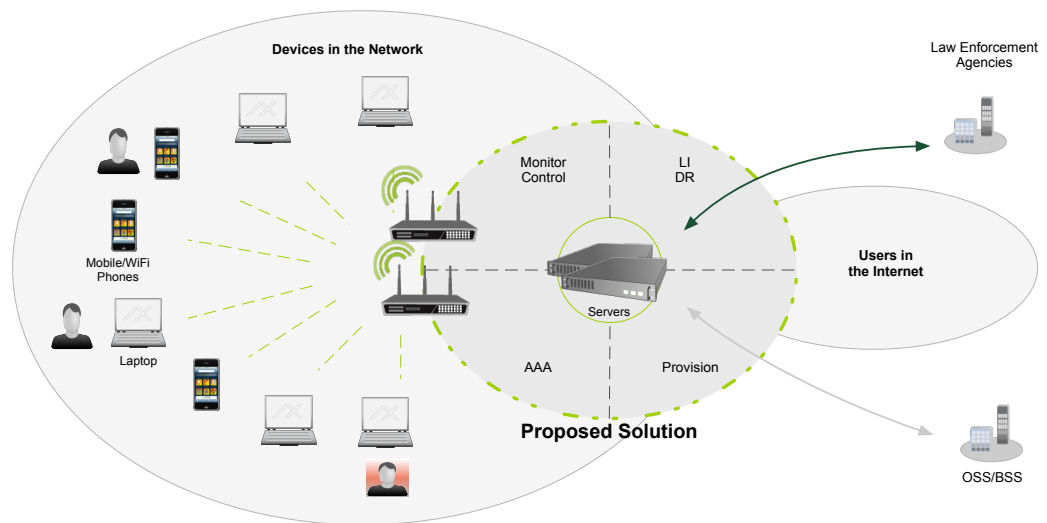
T +49 89 54 99 89 700
F +49 89 67 97 17 07
www.axiros.com
info@axiros.com

In this setup, the subscriber therefore is held accountable for all communication relations of the users in his own network - private IPs are neither accessible to law agencies monitoring Internet traffic nor to LI and DR systems of ISPs. Further, there is no authentication process present for the users in those small area networks. The location retention requirements are fulfilled nearly by definition since the address of subscribers is known to the ISPs and the law enforcement agencies.¹

In large area open access networks the situation is completely different: There is in general no trust relationship between network owner and user *and* the location is not known by default.

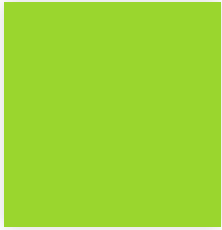
Since network owners can hardly be held accountable for all the traffic the users create, state agencies just *demand* the deployment of “appropriate” equipment to trace back traffic to a certain identity and location of use - but there is no standard describing *how* this should be done.

Within this paper we depict an elegant, robust and scalable design, combining best of breed equipment and software to solve this riddle, enabling the failure resilient operation of large public or enterprise open access WiFi networks in a fully legally compliant way.



Besides premium many features for managed open access WiFi management, like arbitrary authentication sources, bandwidth management and mobility within large WiFi clouds, the solution takes care of IP address management, using scarce public addresses only when a security identified user is logged in and it's offering all required legal interfaces to law enforcement agencies tracing back traffic to physical location and identity of users in the network.

¹ The fact that the subscriber is accountable for all traffic from his own network is commonly accepted and comparable to the fact that also in other areas of daily life parents are accountable for their children and/or employees of small venues are to be trusted by the venue owners.



About **This Document**

Table of Contents / Revision History

meta information

Technical Requirements	5
Deliverables	5
IP and Identity	6
Standard P / Identity Association.....	6
Standard Topology of Open Access Networks.....	7
Identities and IP: The Need for End User Specific Public IP Addresses.....	8
Changing the IP Address at Time of Authentication	10
One to One NAT of the Private Addresses to Public Ones	11
1:1 NAT Northbound of the Access Controller.....	11
1:1 NAT Southbound of the Access Controller.....	12
1:1 NAT on the Access Controller.....	12
Final Solution	13
Final Flow.....	13
Solution Overview and Components Listing.....	16

Revision History

Version	Date	Remarks	Release Status
1.0	05 / 10 / 2006	Initial Version	Public, excl. final flow. Final flow realeased under NDA for partners and customers

Audience

- Architects of Open Access WiFi Networks
- Product Managers

Axiros GmbH

Germany
Rosenheimer Str 30-32
81669 Munich

T +49 89 54 99 89 700
F +49 89 67 97 17 07
www.axiros.com
info@axiros.com



5



6



7



8



9



10



11



12



13



14



15



16