Internet Protocol-based Emergency Services

Hannes Tschofenig

COCOM EGEA, 7th June 2012

Agenda

- Overview, Scope, Design Motivation, and Concepts
- What is EENA NG112?
- Location for Routing and Dispatch
- Security and Privacy

Why do you want IP?

- There are four reasons:

1. Lower costs (commodity nature and competition lowers prices).

2. Lower operational cost compared to legacy infrastructure.

1. Future proof technology: The rest of the industry is moving to IP.

2. More functionality (e.g., multi-media support, data sharing) and extensibility.

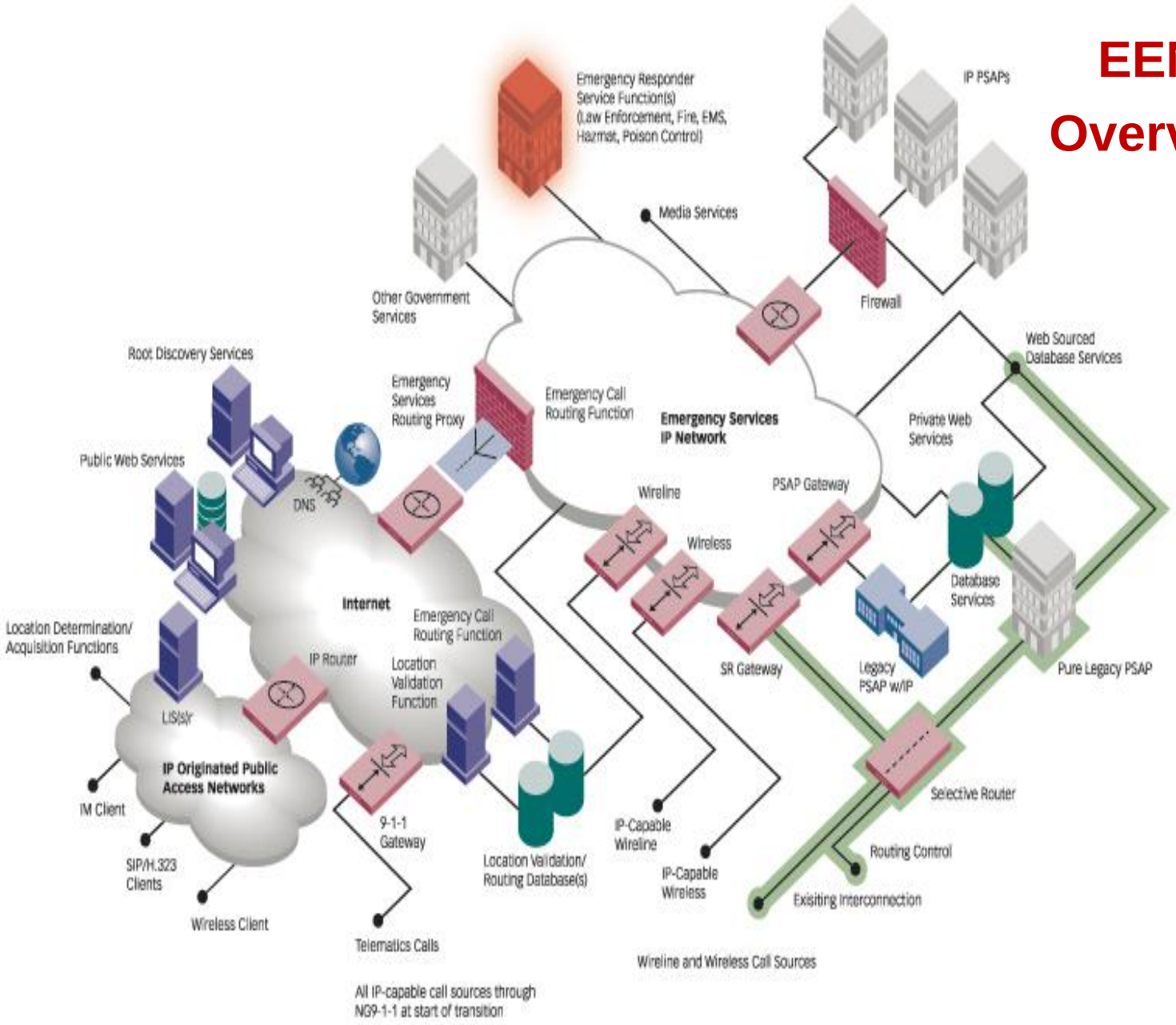
Emergency Services IP network (ESInet)

- Why do you want one?
  - Allow PSAPs to get calls from VSPs and data from location servers.
  - Connect PSAPs among each other.
  - Redundant links for improved availability.
  - Place to put various servers (e.g, firewall for entrance security)
- It’s just an IP network, nothing at all special about the network.
- It’s private and managed but it is not a walled garden.

EENA NG 112 Overview

- The scope of the specification
  - starts with the the Border Control Function (a IP-based application layer firewall) or legacy network gateway, and
  - ends with the PSAP.
- As such, the initial call routing to the edge of the ESINet has already happened.
- Additional call routing may happen within the ESINet and the specification describes this functionality. Examples: overload handling, bridging, routing based on call taker skills.
- ESINet operator relies on external input (e.g., location, emergency call).
- ESINet offers functions to external entities (e.g., routing information).

EENA NG 112 Overview, cont.



NG 112
Overview, cont.

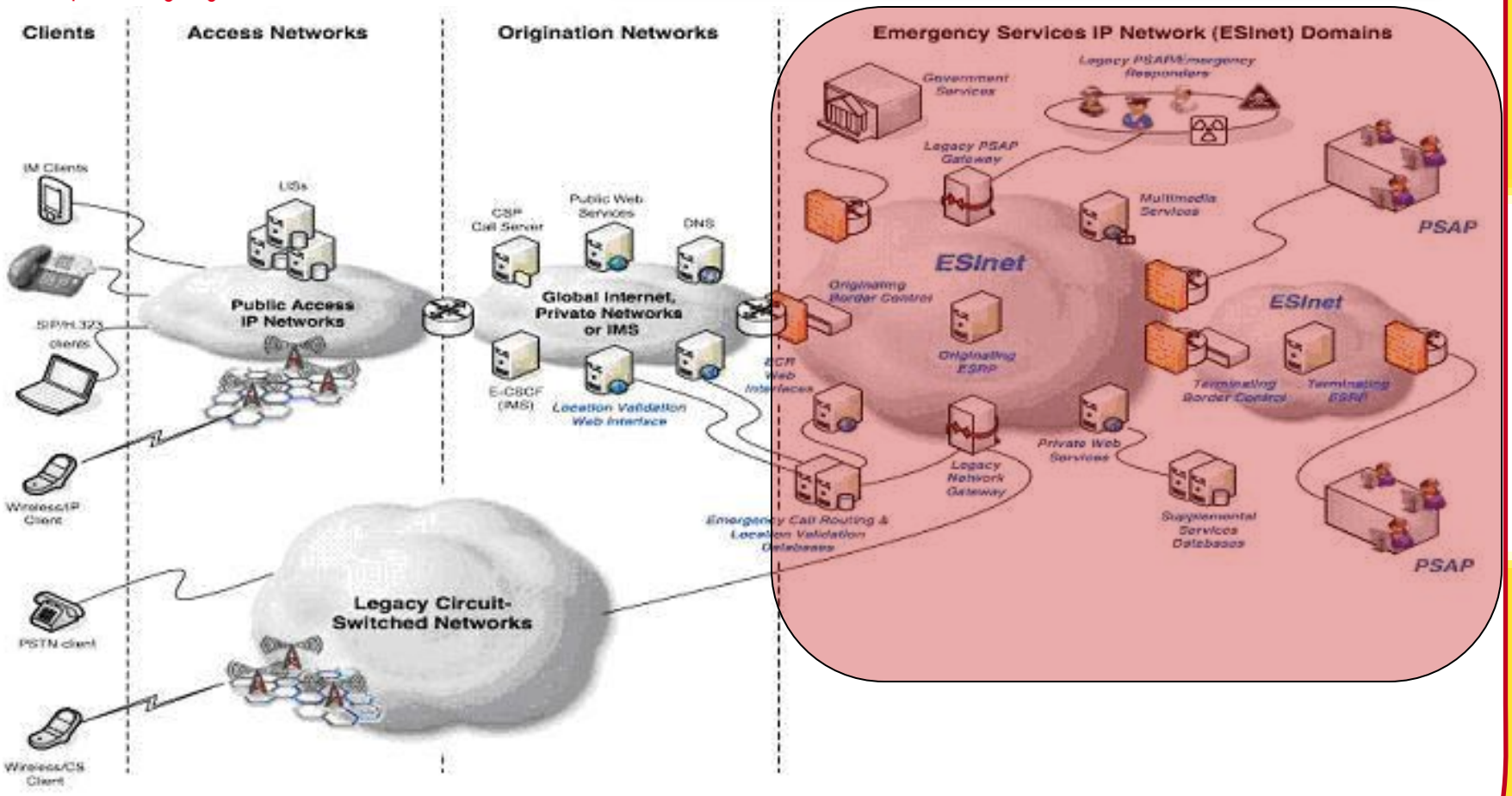
- If you do not want IP-based PSAPs then the NG 112 specification is not relevant for you.

- The NG112 specification helps you to deploy a system that
  - uses international standards (3GPP, IETF, OMA, OGC, etc.) – IP plus SIP & HTTP on top of it, and

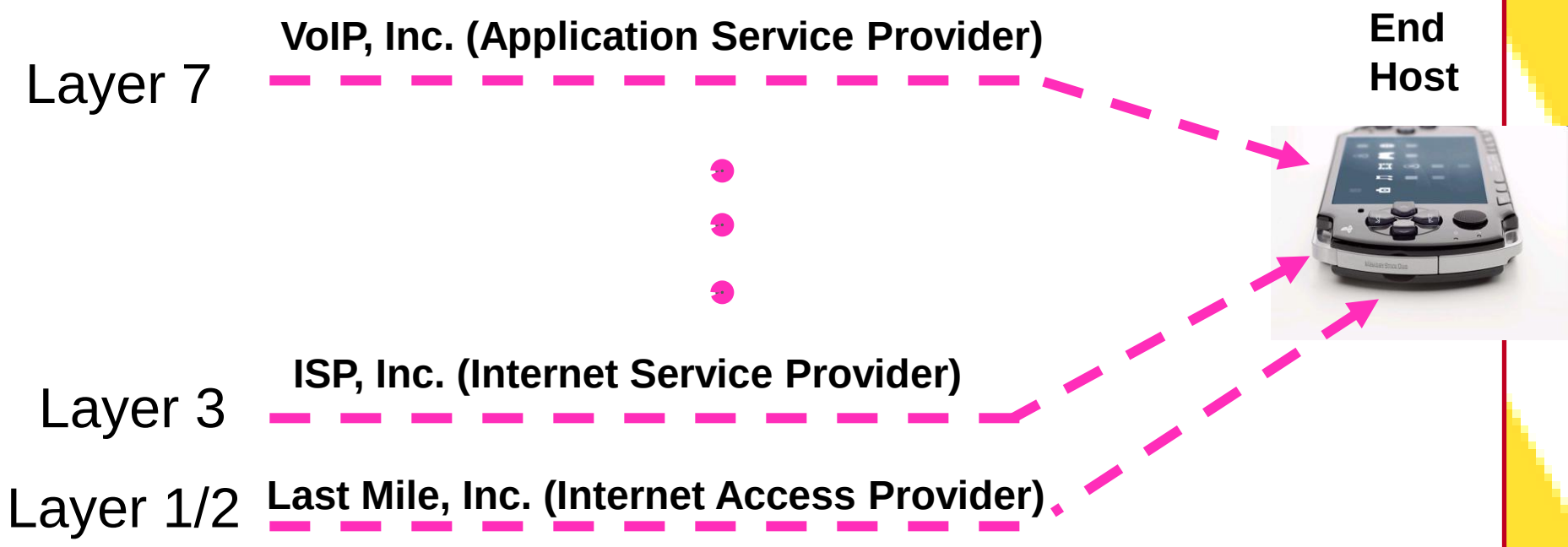
  - lowers vendor lock-in.

european emergency number association

Scope of EENA NG112



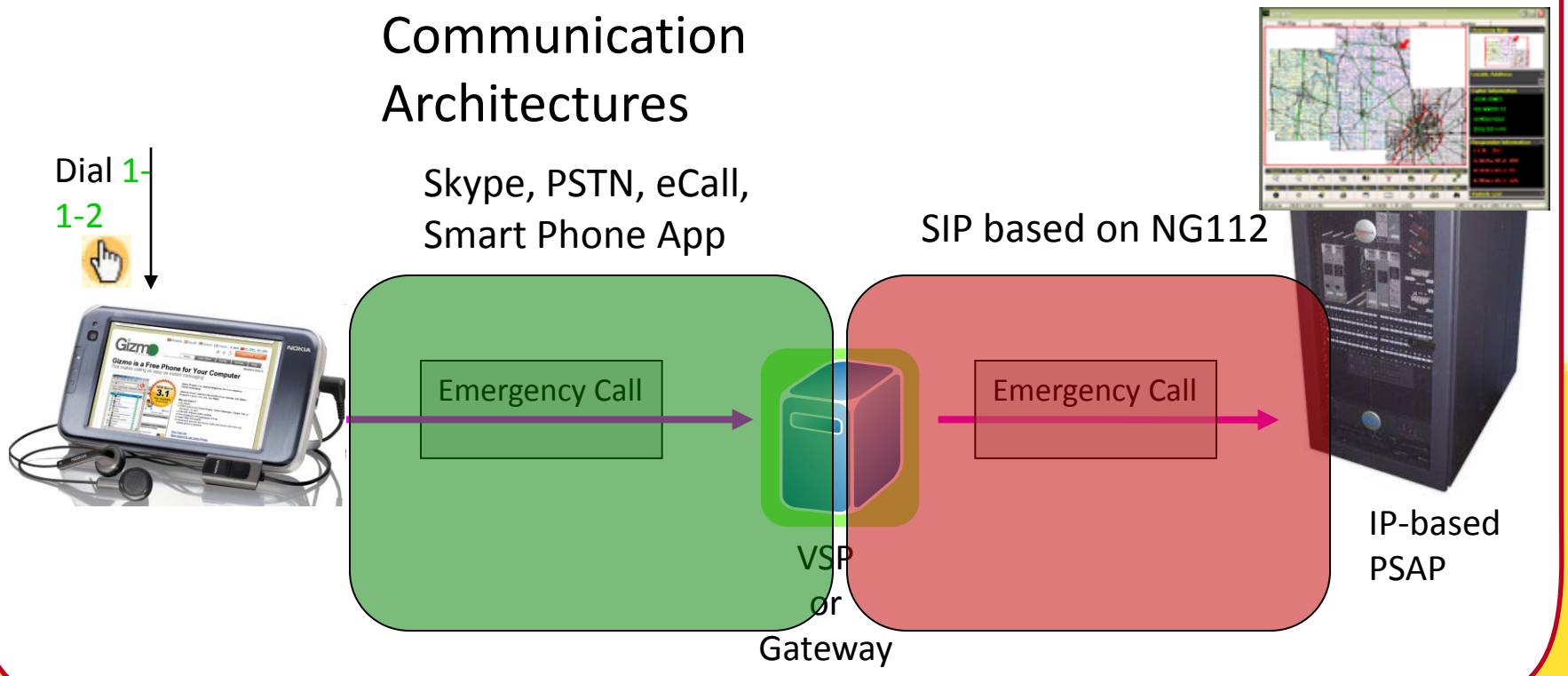
The Layers in the Internet Architecture



Worksplit

- Emergency services build on top of existing communication architectures.
- Standardized communication architectures are available with
  - SIP-based IMS (as defined by 3GPP)
  - SIP-based VoIP (as defined by IETF)
  - XMPP-based IM/VoIP (as defined by IETF & XSF)
  - RTCWeb (as currently work in progress by IETF & W3C)
- Also many non-standardized communication architectures available (e.g., Skype, many Smart Phone Apps)

Interoperability



Worksplit, cont.

- Three features have to be provided by a communication architecture in order to work (failure-free and robust) with the NG112 architecture:
  - (I) Ability to *identifying an emergency call* and to communicate the emergency call to the VSP.
  - (II) Ability to *communicate location and/or a location key*
  - (III) Ability to convey multi-media content (which is the actual emergency communication)

Location

- Two types of usages:
    1. Location for routing of the call to the PSAP
    2. Location for dispatch of first responders.

- Requirements for the two vary considerably.

- Two types of location formats:
    - Civic Location Address
    - Geodetic Location Address

- Location encoding and formats had been standardized long before the EENA work started.

Location for Routing
Three Possible Approaches

(1) Use whatever you have and use it.

(2) Use only those mechanisms that always work.

(3) Don’t use location for routing at all.

Location for Routing Technologies

- End user-based
  - Example: User configures location with VSP when registering for the service.
- Device-based
  - Example: GPS
- Network-based
  - Examples: IP-to-geolocation databases, ISP-operated location servers
- Network-assisted
  - Examples: SSID/Cell ID databases, A-GPS support

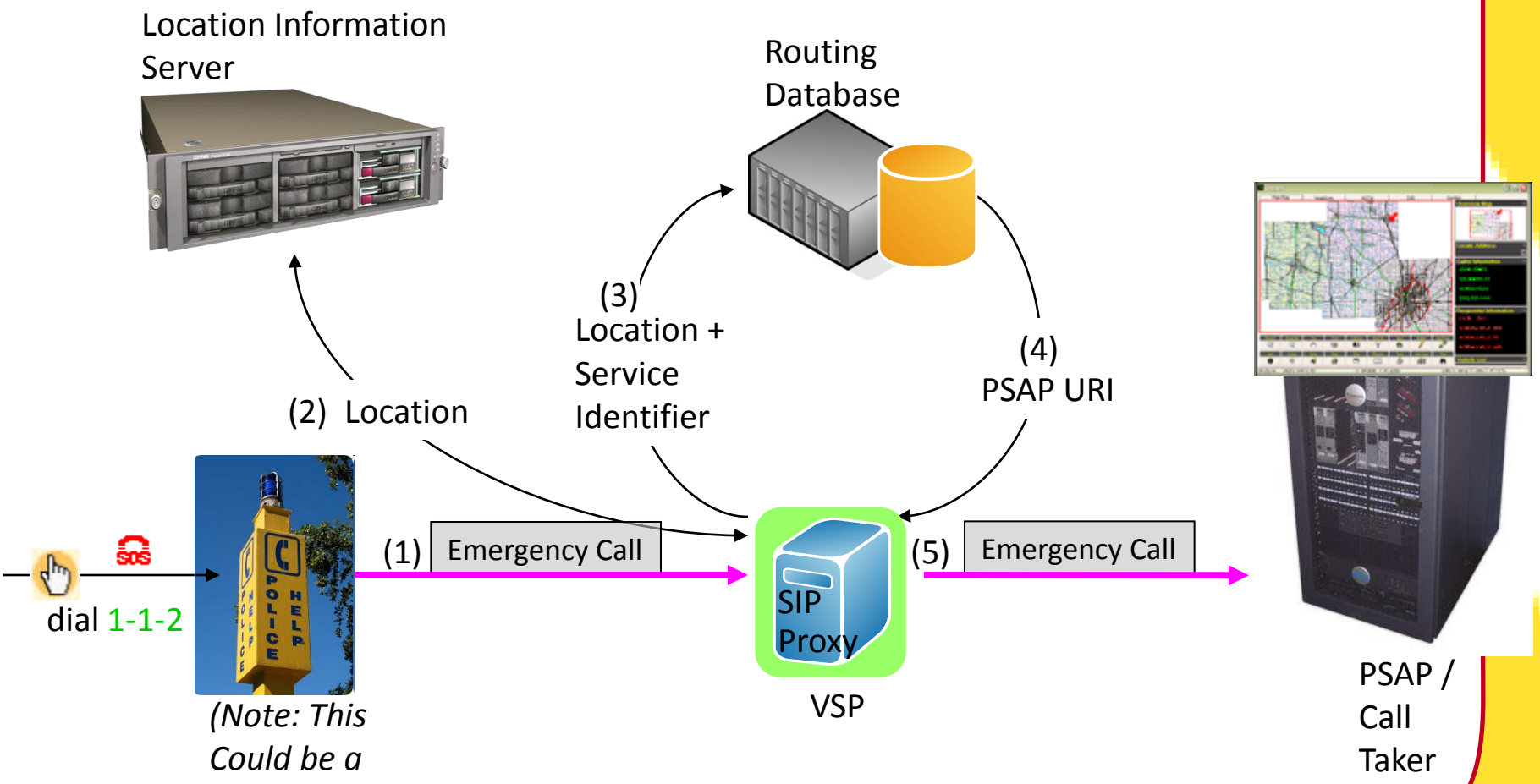
Emergency Call Routing
Main Options

I) End host driven Model
- End host obtains location
- End host triggers resolution (which also provides information about the supported emergency services numbers)

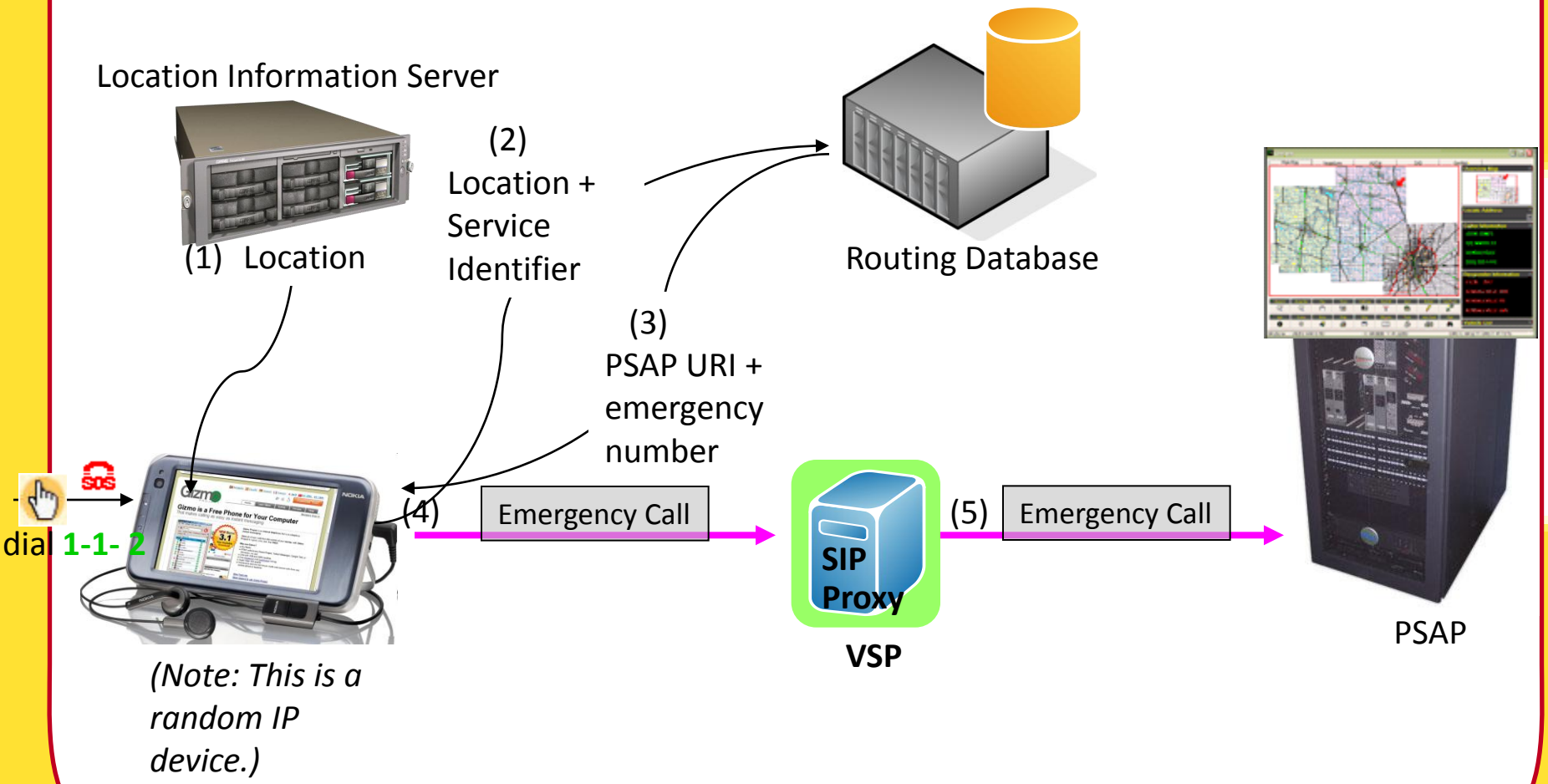
II) Proxy driven Model
- VSP obtains location
- VSP determines ESRP/PSAP.

- Various variants possible and described later.

Emergency Call Routing
Proxy driven Model



Emergency Call Routing
End Host driven Model



Emergency Call Routing Variations

A) Single PSAP or PSAP operating for the entire country.

In this case the granularity of the location information only needs to be on a country level. This can easily provided by many of today's location based services (e.g., IP-to-geolocation).

Example: UK

Emergency Call Routing Variations, cont.

B) Emergency Services Routing Proxies
(with many PSAPs per country)

Only country-level location granularity is needed to find one of the ESRPs. ESRPs can (automatically and without human involvement) retrieve more accurate location from ISPs/IAPs, when needed.

Example: Variation of the Swedish deployment. German eCall approach in HeERO project.

Emergency Call Routing Variations, cont.

C) ISPs provide Rough Location to End Hosts (for routing only)

The level of provided location information depends on the number of PSAPs. Solution described in IETF ECRIT WG.

D) ISPs provide ESRP URI (instead of location) to end hosts.

This allows the VSP to route the call to the nearby PSAP based on the provided URI.

Location For Dispatch Approaches

Choices are limited for robust location determination:

- LIS discovery is done by end host.
- VSP functionality is provided by the ISP and routed there directly (as it is done with IMS).

european emergency number association

Emergency Calling
Further Challenges

- How to ensure that the emergency services infrastructure does not become vulnerable to security attacks (DoS)?
- Directive 95/46/EC provides the baselines data protection rules for European member states.
  - Exemptions exist for emergency services
  - Still: How do we ensure that location information is only obtained for emergency calls or otherwise authorized by users?

Emergency Calling Security

- Think about the type of threats you want to protect against.
  - EENA NG112 has an extension security chapter discussing threats.
- Resource consumption at the PSAP based on false calls is one biggest security threats:
  - See also EENA publication on this topic: http://www.eena.org/ressource/static/files/2011_03_15_3.1.2.fc_v1.0.pdf
  - Note that we are now focusing on location for dispatch – not for routing.
- Many of the reasons for false calls cannot be "solved" via technical means only.
- Note: Problem is not unique to IP-based emergency services. Legacy networks also suffer from these problems.
- The existence of malware botnets has to be considered as well. (not just a theoretical threat)

The Attribution Problem

- Attribution …
  - Requires to identify the agent responsible for the action
  - Determining the **identity or location of an attacker** (or an attacker's intermediary).
- Four aspects of attribution:
  - Types: if users are expected to be identified in some way, what is the source of that identity, and what can we conclude about the utility of different sorts of identity?
  - Timing: what are the different roles of attribution before, during and after an event?
  - Investigators: how might different parties exploit attribution as a part of deterrence?
  - Jurisdiction: what are the variations that we can expect across different jurisdictions, and how might this influence our choices in mechanism design?

(*) D. Clark, S. Landau, "Untangling Attribution", in Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing, 2010.

Types of Identity

- Goal: real-world identity of the emergency caller
- Can only be obtained via resolution steps:
  - SIP AoR and resolution via VSP
  - IP address and resolution via ISP/IAP
  - Entirely independent mechanism (which does not yet exist, like emergency service certificates).
- Requires in-person identity proofing (and higher level of assurance infrastructure) during user registration.

Emergency Call Routing Security

- Physical location of adversary may help PSAP call taker in decision making.
- Spoofable to a certain degree since the location configuration steps are vulnerable to manipulation.
  - Particularly true for location determination techniques that provide better location accuracy.
- Focusing on network provided location rules out many practical deployments.

Emergency Call Routing Timing

- Before the Fact: Prevention or degradation
  - Example: Disallow SIM-less emergency calls
- Ongoing: Attribution as a part of normal activity
  - Example: Education about cost of emergency services infrastructure.
- During the Fact: Mitigation
  - Example: Signal ‘false call’ warning to caller.
- After the Fact: Retribution
  - Example: Take person to court.

Emergency Call Routing
To tackle

- Challenges to overcome:
  - identity proofing is expensive
  - problems with different jurisdictions being involved
  - Traversing links from digital identity to real-world entity and physical location is difficult (and chain easily breaks)
  - Knowing the location of the adversary does not immediately lead to the real-world entity
- There are non-technical challenges and solutions as well.

Emergency Call Routing
Privacy

- Only the emergency caller knows that it is making an emergency call.
- By dialing the emergency call number he / she implicitly consents to release of location information.
- Allowing end devices to ask for location information and providing that information is not a problem for privacy.
- Solutions where location information can be retrieved without any emergency call taking place are problematic.
  - Example: Imagine a VSP being able to query precise location of a user without user consent.

Conclusions

- We recommend to design for global interoperability to accomplish the economic benefits and to support citizens.
- Location for call routing:
  - Various deployment models possible.
  - Suggestion to consider practical approaches as well since existing deployment can be leveraged.
- Location for dispatch:
  - Requires cooperation between the ISP/IAP and the end host for LIS discovery and retrieval of a location key.
  - Time to get better location with higher accuracy ?!
- Security and Privacy
  - Attribution requires location or identity of the adversary. Do not only focus only on location since it will not cover all the threats.
- Start with small deployment since the number of VoIP emergency calls will be low at the beginning.