



# NGN Security - Evolutionary Security Standards

Judith Rossebø  
Telenor R&D  
TISPAN WG7 Chairman  
[judith.rossebo@telenor.com](mailto:judith.rossebo@telenor.com)



# Overview

- ❑ **ETSI TISPAN**
  - **WG7 security**
- ❑ **ETSI NGN security**
  - **Security goals for the NGN**
  - **Challenges and threats**
- ❑ **ETSI NGN Security Standards**
  - **Where we are now...**
  - **Future plans**
- ❑ **Conclusions**

kst1

NGN?

ETSI?

kst; 2005-09-20

# What is ETSI TISPAN?

**TISPAN:** Telecommunication and Internet  
converged Services and Protocols for  
Advanced Networking

**NGN:** Next Generation Networks

**TISPAN NGN:** Converged Fixed-Mobile solutions

A significant step has been taken to enable the Multimedia Fixed-Mobile Convergence in TISPAN NGN Release 1

## WG7 security:

TISPAN Working Group (WG) 7 is responsible for the management and co-ordination of the development of security specifications for TC TISPAN.

- For TISPAN NGN Release 1, TISPAN WG7, assisted by the specialist task force STF292, has:
  - Defined security requirements;
  - Defined a security architecture for NGN R1;
  - Conducted threat and risk analyses for specific NGN use cases;
  - Proposed countermeasures.

WG7 security standardisation is risk-based:  
Using the STF292 methodology for Systematic threat, vulnerability and risk analysis (TVRA)

# TISPAN NGN fixed-mobile convergence

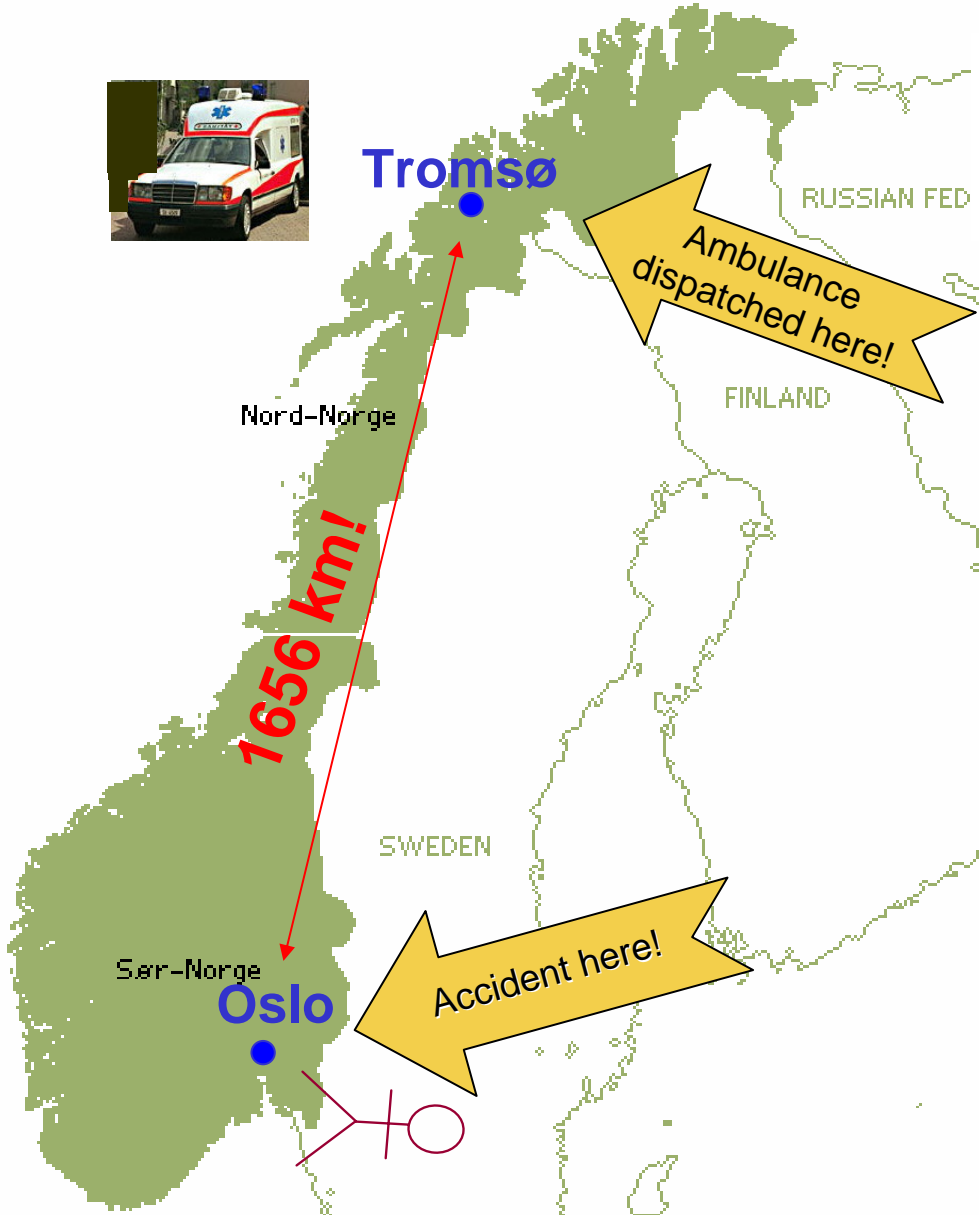
- ❑ ETSI TISPAN proposes an architecture basis consisting of a range of subsystems:
  - Access network attachment subsystem
  - Resource and admission control sub-system
  - IP Multimedia Subsystem (IMS) (from 3GPP)
- ❑ TISPAN is collaborating with 3G to enable IMS over fixed networks
  - To coordinate the IMS evolution and resolve issues
- ❑ When applicable TISPAN re-uses 3G specifications
  - in a process of endorsement where IMS is jointly developed

 *cooperating with*

  
A GLOBAL INITIATIVE



# The Next Generation Network will provide:



# Goals for NGN Security

- ❑ **Prevention of masquerade**
  - Checks who the users really are
  - May be used to limit fraud
  - May be used to raise trust (confidence)
- ❑ **Privacy of communication**
  - Regulatory requirement
  - Customer expectations
- ❑ **Availability of the NGN services**
  - Regulatory requirement (sometimes)
  - Customer expectation



# Constraints

## ❑ The regulatory environment

- Support of citizen
  - Emergency call services
  - Lifeline services
- Support of privacy directive
  - Call tracing
  - Malicious communication identification
- Support for law enforcement
  - Lawful Interception

## ❑ Legacy networks and equipment

- Strong security mechanisms may not be applicable – how do we mitigate at lowest cost?



# Threats and challenges to a secure NGN?

- ❑ Legacy Fixed and 2G/3G security is fundamentally different:
  - Authentication
  - Confidentiality/Integrity
- ❑ xDSL relies on some of the assumptions of legacy fixed
- ❑ Far-end NATs used in fixed IP-based networks, but not in 2G/3G
- ❑ Use of WLAN in home networks



## Security in legacy fixed networks:

### ❑ Traditionally relies on physical control:

- **No explicit authentication of terminals**

- Terminal is assumed to be fixed in a location
- Owner is contractually bound to pay for calls
- In most cases, the individual responsible for the bill is collocated with the terminal.

### ❑ Full IMS requires explicit authentication

- **new costs for existing fixed deployments**



# Security in 2G/3G networks:

- ❑ **ISIM/USIM over UICC for:**
  - **Strong authentication**
  - **Encryption**
    - Confidentiality of media
    - Confidentiality/integrity protection of signalling
  - **Tamper-proof means of carrying identity**
- ❑ **Cost of explicit authentication is already built in (since 2G)**

**For 3GPP IMS these mechanisms are reused:**

- ❑ **So no added costs**



# Threats: Previously

Focus on assets belonging to :

**Single National Operator**

Featuring:

Voice services

Often single-vendor

Now:

**(Multiple) Network Operators**

**End-Users & Applications**

**Service Providers**

**Natl. & EU. Regulatory Authorities**

multi-Services / Internet etc.

multi-vendor

# WG7 security – Current focus:

- ❑ New threats and risks landscape
- ❑ Authentication to IMS
  - Solution for legacy deployments
    - Access to IMS granted based on access network authentication (NASS-IMS bundled)
  - ISIM over UICC otherwise
    - Reuse of IMS mandates this
    - Challenge – realising use of ISIM over UICC for access to IMS (from any terminal – not just 3G terminals)....
- ❑ NGN (security) protocols must work in presence of far-end NATs

# Status of WG 7 security work

## □ Release 1:

- **NGN R1 Security Requirements, WI 07014**
  - TB approved in December 2005
- **NGN R1 Security Architecture, WI 07017**
  - WG7 approved in December 2005
- **NGN R1 Threat and Risk Analysis, WI 07016**
  - WG7 approved in December 2005
    - PSTN/ISDN Emulation System Security analysis
    - Threat analysis for IMS-NASS bundled authentication mechanism
    - WG7 approved in December 2005
  
- **NGN Lawful Intercept (LI), WI 07013**
  - Ongoing cooperation with TC LI and liaison with 3GPP SA3 LI
  - WG7 approval expected in April, 2006

## □ Release 2 and beyond:

- Continued focus on threat and risk analysis, requirements, and architecture
- New WI NGN Countermeasures planned



## Status of WG7 security work #2

### ❑ Security standardisation methods

- Threat Vulnerability Risk Analysis (STF292)
- Assurance techniques (STF292)

### ❑ Security guidelines

- Deployment (STF292)
- IPsec (STF292)
- Keying (STF292)

# Overview of TISPAN Plans

- ❑ NGN Release 2 planning has not yet started
- ❑ Interest in following challenges for R2 and beyond:
  - Continued work on authentication to NASS and to IMS services:
    - HW-based ISIM (UICC/USIM) and/or
    - Equivalent and/or
    - SW-based ISIM authentication,
  - Single-sign on/ID Management
    - Various, unique identities in the NGN environment
  - Emergency services issues
    - (authentication, authorisation, location ID)
  - Interworking of various security mechanisms
  
  - Cooperation with AT NGN@Home
    - Residential gateways
    - Home networking security
    - NGN Terminal security (?)
  - Cooperation with ECMA
    - Corporate network NGCN security interactions with NGN

# WG7 security - Conclusions

- ❑ TISPAN WG7 is addressing NGN security
  - New risks
    - an IP-world...
    - a large legacy base...
    - diversity of access and terminals...
- ❑ ETSI TISPAN WG7 is addressing the threats and challenges for securing the NGN
  - Systematic threat, vulnerability and risk analysis (TVRA)
  - Based on the results of the TVRA countermeasures are being standardised
- ❑ ETSI TISPAN NGN security standards are helping to enable fixed-mobile convergence



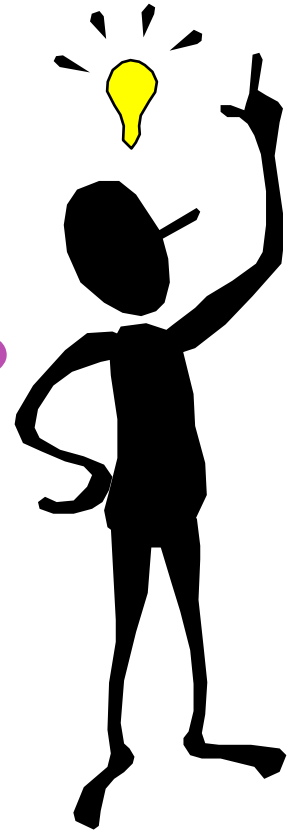


***THANKS FOR YOUR ATTENTION***

**Questions/Comments ?**

**ETSI TISPAN Portal:**

[http://portal.etsi.org/Portal\\_Common/home.asp](http://portal.etsi.org/Portal_Common/home.asp)





## For more information

- ❑ **European Telecommunication Standardisation Institute [www.etsi.org](http://www.etsi.org)**
- ❑ **TISPAN security specialist task force leader [scott.cadzow@etsi.org](mailto:scott.cadzow@etsi.org)**
- ❑ **TISPAN security working group chair [judith.rossebo@telenor.com](mailto:judith.rossebo@telenor.com)**