Trusted services in Luxembourg

1st Luxembourgish Workshop on Location-based Services and Privacy Assurance (LSPA)

04/02/2011

Dr. Carlo Harpes
itrust consulting
harpes@itrust.lu

Agenda

- Context and Privacy threats
- User requirements
- Location Assurance Service Provider
- Security Approaches
  - EuroPriSe
  - Product Security
- Outlook

Objectives

- Foster discussion on security issues of Location-Based Service (LBS)
- Explain privacy issues in our projects, e.g. LASP

Context

> Growing Location-Based Service

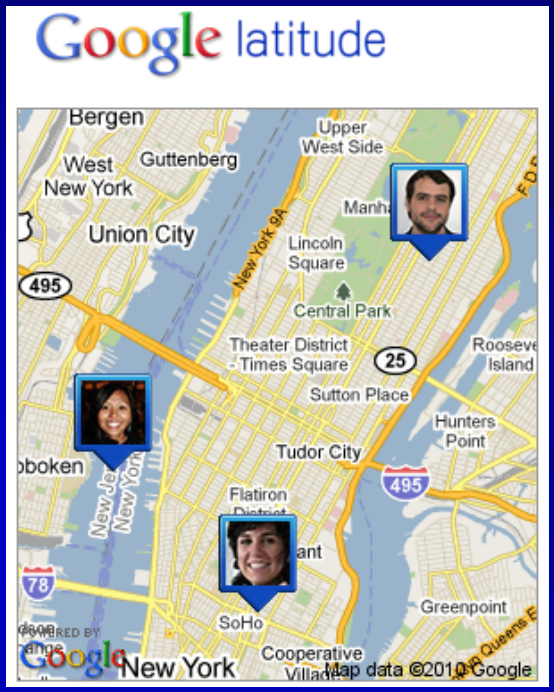
Many free services

Geo-tagging

- on each iPhone, e.g.
- on Picture sites on the web

New services very easy to make

- built on free service Google Map and GeoAPI
- cf itrust-foetz.servehttp.com\Alidade

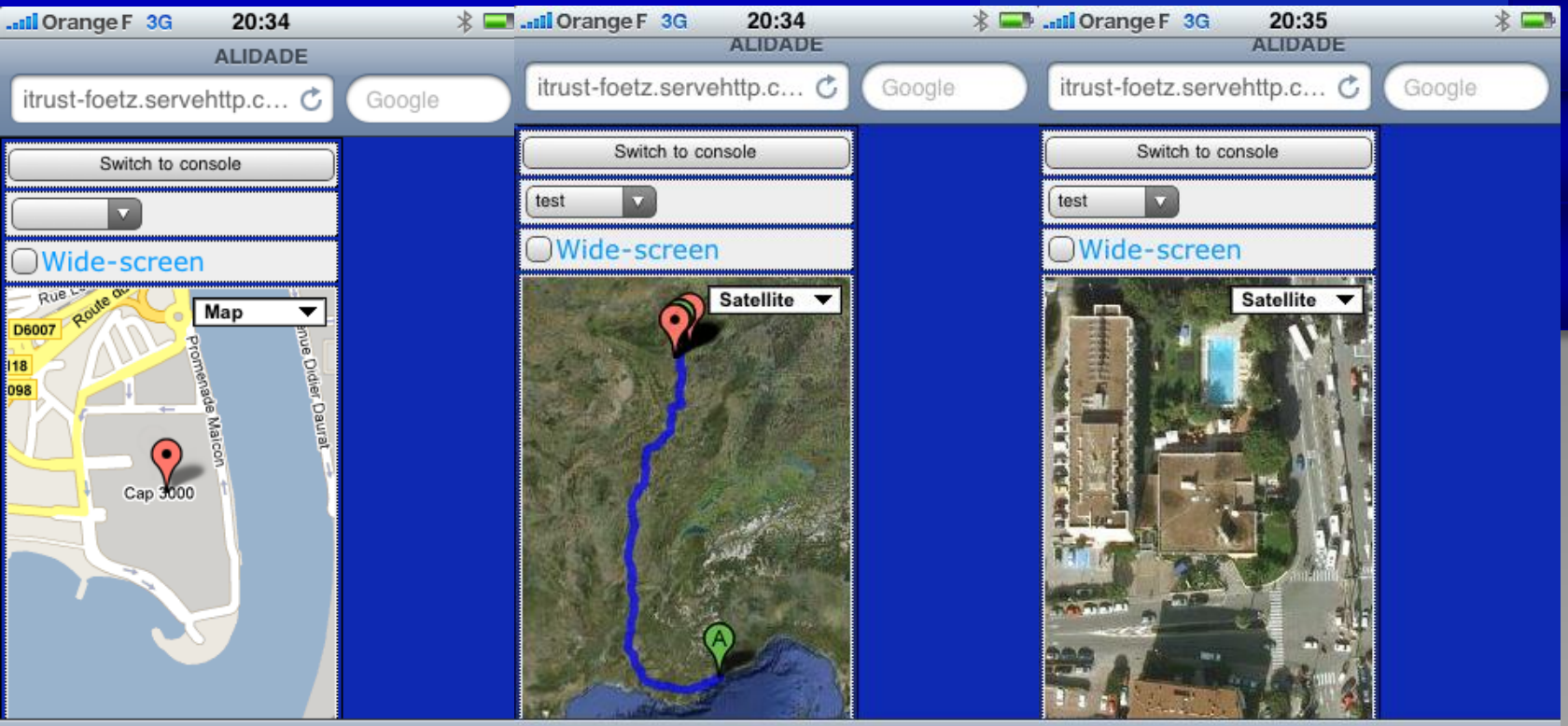


Context

> Growing Location-Based Service

New service very easy to make

- built on free service Google Map and GeoAPI
- takes less than a week
- cf itrust-foetz.servehttp.com\Alidade



Context

> Little, but growing privacy awareness

No real care on passwords and shared information

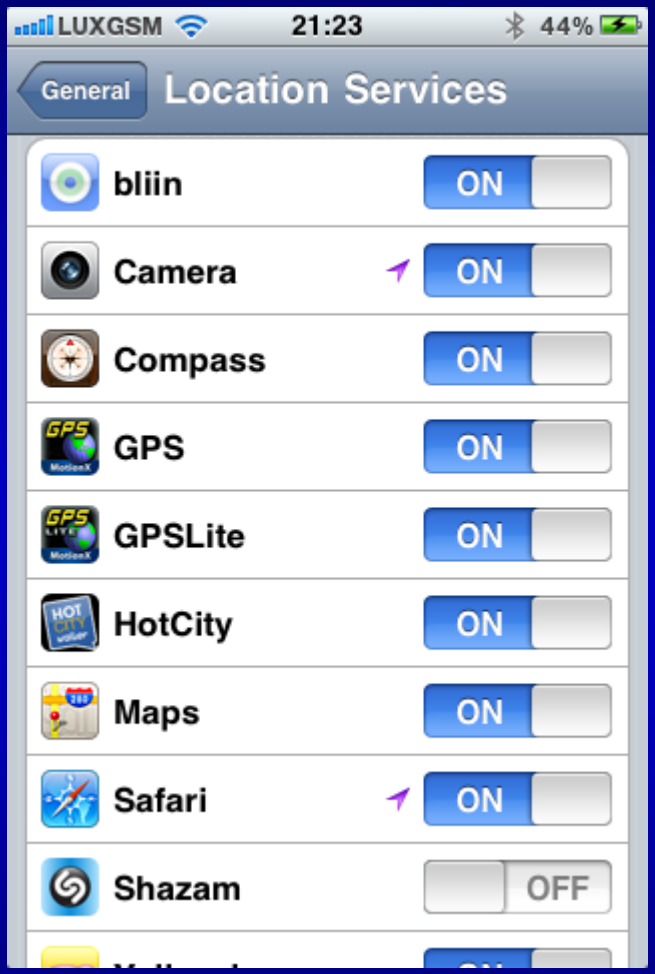
- Social engineering for password very easy
- Very private info are shared with the entire world,
- cf www.cases.lu

Concerns by data privacy authorities

- Opinion 5/2009 on online social networking (01189/09/EN WP 163):
  - No search on location without explicit consent,
  - access to near members is critisised.
- Cf www.cnpd.lu, ec.europa.eu

Context

> … resulting in lots of information



Context

> Challenging questions

Is the user ready to pay for better privacy and security ?

How to build this security ?

How to get users trust in this security ?

Context

> Privacy options

Client-based

- The user computes his position.
- e.g. GPS
- easier to secure than…

Network-based

- Ex: iPhone: a service provider Skyhook tells you the location of the WiFi antenna next to you
- This provider has the possibility to trace users, abuse or sell data…

- Should we trust such service providers ?
- Do we have a choice ?
- Better: When can we trust?

User requirements

> Demo at Galileo Application Days (1/2)

Based on demo and questionnaires

On March 2010, in Bruxelles
Not representative,
feedback from 32 questionnaires:

Functionalities

People want to have a

- fast and easy to handle service
- with high accuracy (~1 meter (38%), ~10 meters (44%)),
- which could be installed on the most popular mobile phones.

Price

OK for commercial service (73%),
with cost between 3 and 5 Euro per month (34%).

Target use is the family environment

for localisation of their young children (40%) and of their elder family members (21%)

User requirements

> Demo at Galileo Application Days (2/2)

Main obstacle

- concern that data could be shared with other parties (39%),
- concern that they can get localised without their consent (31%)

Requirements

- data to be stored securely
- operator be put under supervision of a Data Protection Authority (66%),

-> people have large concerns on their privacy.

Interpretation

- in contradiction with the current popularity of unsecured social networks, and the willingness of peoples to share very private information.
- But it is consistent with the current public debates and the raised concerns on privacy issues.

User requirements

> Current situation

Increased awareness for privacy

- Thanks to Facebook, Google StreetView
- Confirmed at the CNPD Conference:

Business Case

- In EU, 90 Million GPS handsets by 2012.
- LBS enable smartphone low penetration in EU compared to the world.
- ABI Research: market for wireless location-based applications is expected to reach $14.5 Billion in 2014.
- Local advertising market is estimated to be $150 Billion in the U.S. alone"
  http://www.indoorlbs.com/search/label/indoor%20location

LASP

Project description

Location Assurance Service Provider

ESA Project by itrust consulting and University of Luxembourg

2010-2012

Objectives

Specify and implement a prototype of a localisation authority

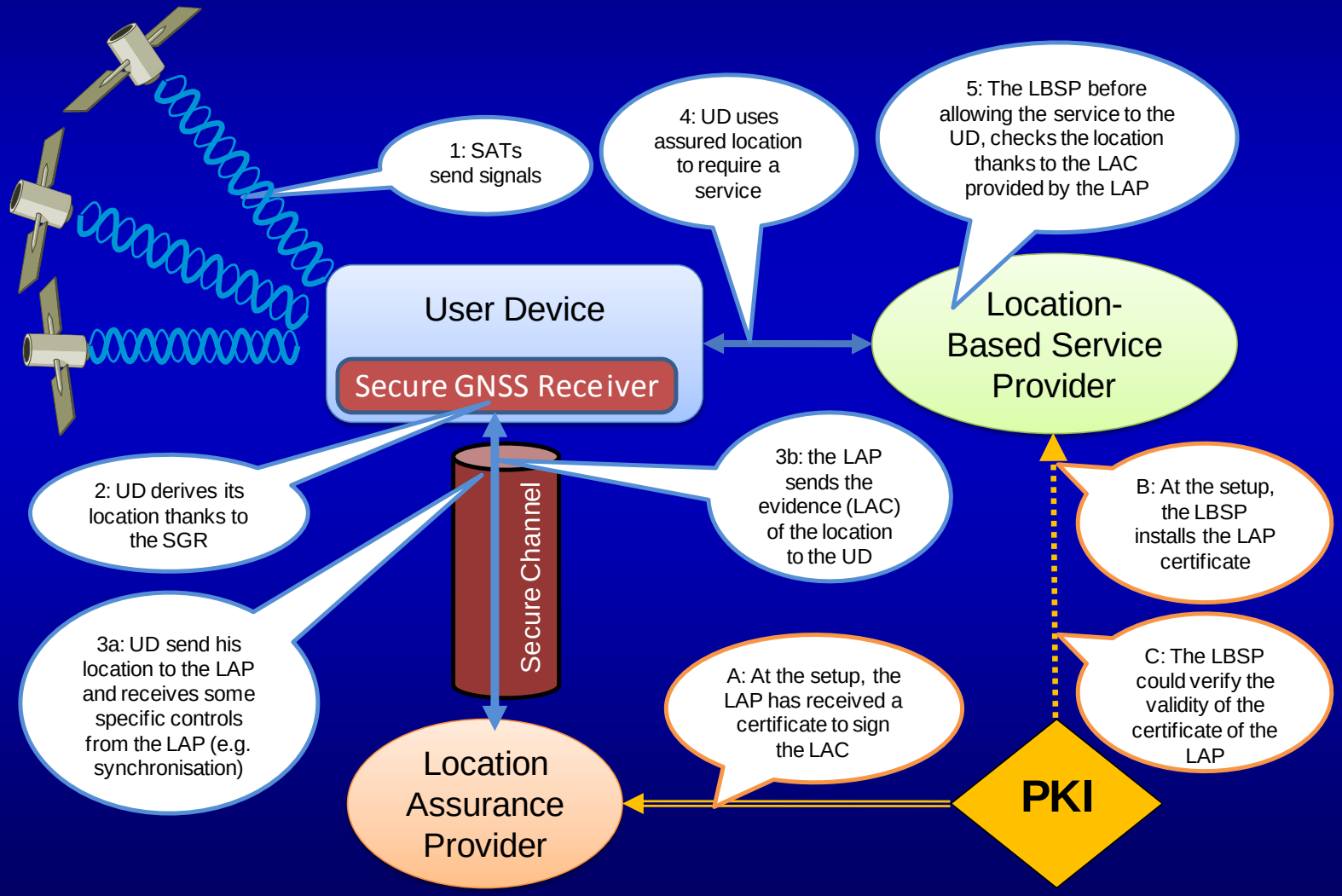
- Performing security checks before certifying a localisation
- Demonstrate service and communication between LAP and devices to assess the user location

Consider privacy issues (like anonymity) for privacy-enhanced services

Deploy and dissemine the service

LASP

Service Architecture



Security Approaches

Overview

Product Security:

- ISO 15408 Common criteria

Process Security:

- ISO/IEC PRF TR 19791

Information Security Management System:

- ISO/IEC 27001 ISMS – Requirements
- ISO/IEC 27002 ISMS – Code of Practice…
- ISO/IEC 27006 ISMS – ...Certification

Privacy standards:

- ISO 29100 Privacy Framework, …
- ISO 29190 Privacy capability assessment framework, …

Labels

- Selon les réflexes CASES
- EuroPriSe (European Privacy Seal)

EuroPriSe

Overview

Definition

EuroPriSe (European Privacy Seal)

What is it?

Transparent European privacy certificate that fosters

- consumer protection & civil rights;
- trust in IT;
- privacy by marketing mechanisms.

Source:

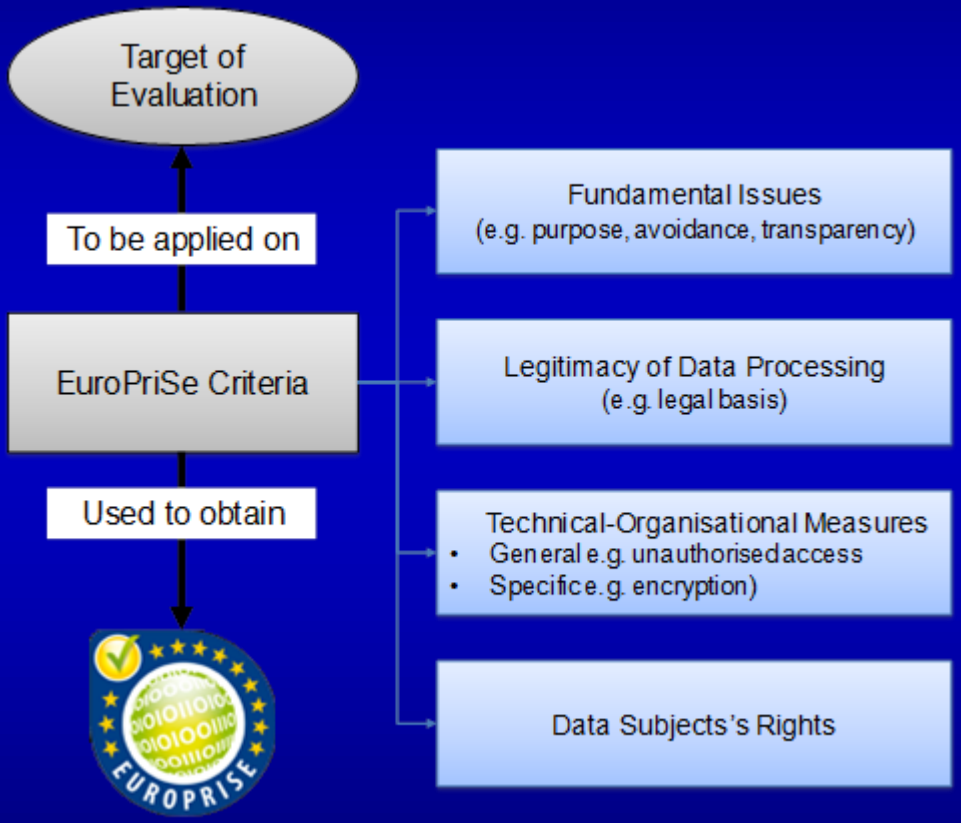
www.european-privacy-seal.eu

Owner:

Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein

EuroPriSe

Overview



Product Security

What is ISO 15408?

CC = Common Criteria

= an internationally standardised collection of criteria for the evaluation of security related products
http://www.commoncriteriaportal.org/

CC (ISO 15408) consists of three parts:

1. Introduction
2. Security Functional Requirements
3. Security Assurance Requirements
   (CEM = CC Evaluation Methodology
   = instructions for the evaluator how to verify the developer's compliance with the criteria)

Usage here

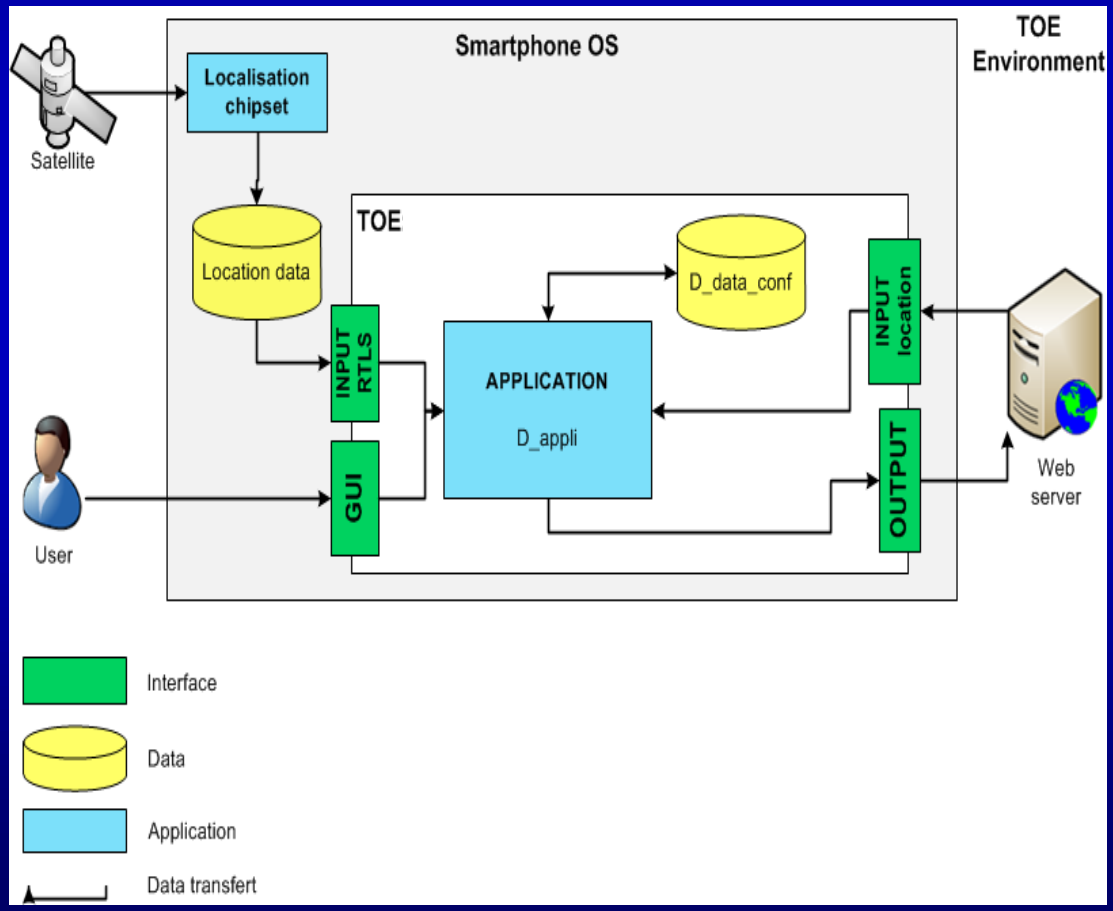
- Part 2 to design and document secure LBS in full transparency
- Later: certify that it is secure in the conditions that it has been designed for.

Product Security

What is ISO 15408?

Protection Profile

= security profile for a product called Target Of Evaluation



Product Security

TOE description

TOE type:

- Software software component for different devices such as Smartphone.
- Read location information of GPS chipset
- Send it regularly to a web server.
- Retrieve location of others from web server.

Usage:

- collect and send location data about people

Security objectives for operational environment

- The correct operation of the TOE depends on
  - the operating system on which it is installed,
  - on the hardware,
  - on the visibility of satellite signals, and
  - on the GSM network for external communication.

Product Security

Assets and threats

Assets:

D_Data: Location data which are transferred through the application from the GPS chipset to the web server.

D_Data_Conf: Configuration data of the application.

D_Application: The application which is installed on the smartphone.

Threats:

T_Confidentiality: Access to the location data by an unauthorized person or program by listening to the message or by accessing to configuration data through a second application. On data and config

T_Integrity: Modification of the application configuration. The application can be modified to send location data to a wrong server or to send wrong location data.
On data and config, not applic. as OS not under control

No availability as very hard to handle formally !

Product Security

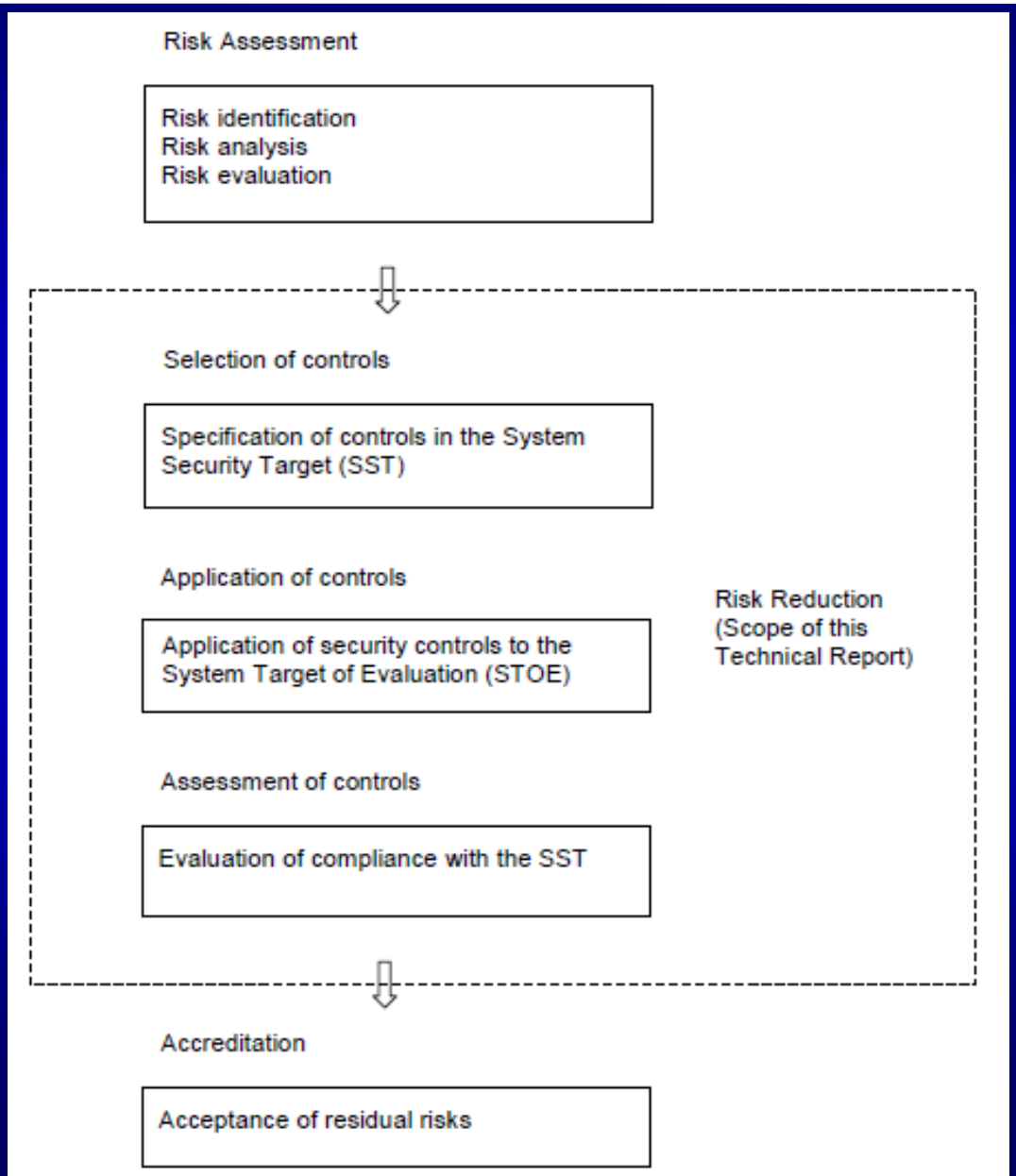
Concerns for the design

Security objectives of the TOE :

- OT_Confidentiality: The location data has to be protected against access from unauthorized person.
- OT_Software_Integrity: The application should not be modified by a malware or an unauthorized person.
- OT_Data_Integrity: The data send by the software should not be manipulated before reception by the web server and vice versa.
- OT_Configuration_Integrity: The password should not be modified by an unauthorized person.

Process Security

Overview ISO TR 19791 (Draft!)



Conclusion

And open questions

Findings:

- It is easy to develop (unsecure) LBS.
- Users want security and require supervision of Service provider
- We recommend transparent security design and commitment to a protection profile.
- We defined a high-level model for general LBS security.
- Service provider should be prepared for certification or at least labelisation.

Challenges:

- Do security that the user is willing to pay.
- No control on global player (Google, Skyhook),
  - But they have a reputation to defend !
- No control on OS (iPhone, e.g.)
- -> considerable limit on the final privacy that a local service provider can ensure.

Questions & Discussion…

Thank you for your attention

Carlo Harpes
harpes@itrust.lu

About itrust consulting

> Activities

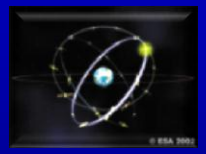
(1) Management consulting

(2) Security consulting

Risk Analysis:
- Value model
- Safeguard evaluation
- Risk map
- Risk status
- Deficiencies report

Computer Forensics

Audit



Crypto ← **Protocoles**

Classification

SE	VIT	7 6
CO		5
RE	IMP	4
IN		3
PU	NOR	2 1

(3) Technical (and security) design

(4) Training and awareness

About itrust consulting

> Services

Consultancy

- ESA Studies LuxLAUNCH
- Security policies
- Information risk analysis

Audit

- Web Banking
- Proces certification
- Malware analysis
- ISO 27001,
- ISO 15408...

R&D – Technical and security design

- ESA: Secure Galileo localisation
- Incident manager
- Celtic, FP-7
- Risk Management Tool TRICK-Light

Multisourcing

- Security officer assistance
- SME security support (in preparation)

About itrust consulting

> Experiences of a research-making SME

Research in the strategy of itrust consulting

Acronym for
"**I**nformation : **T**echniques and
Research for **U**biquitous **S**ecurity and **T**rust"

Strategy:
from pure consulting to
mix between security design, support,
and consulting.

Past experience:
Essential support to sustainable growth in 2009:
6 employee with permanent contracts

Tactic:
Maintain high rate of R&D
in the next 3 years