3GPP TSG SA WG3 Security — S3#25 **S3-020478**
8 - 11 October 2002
Munich, Germany

LIF#8 Meeting LIF/SIG#10(02)-059
17-19 September 2002
Vienna, Austria

TITLE – LS to 3GPP TSG WG CN4, CN, SA3, SA2, and GSMA SerG on the protocol development for the GMLC Lr-interface

SOURCE –LiF SIG

AGENDA ITEM –

LIF SIG would like to thank 3GPP TSG CN, TSG CN4 and TSG SA2 for delegating the task of developing the inter-GMLC interface to LIF.

The development work of the MLP-based Lr interface has already started within the LIF SIG-Roaming Ad-hoc group. This work takes into account the changes that have been introduced in 3GPP TS 23.271 during SA2#25 and SA2#26.

We expect the protocol for the Lr interface to be ready by March 2003, as requested by SA2, depending upon completion of the stage 2 specifications in a timely manner.

As the LIF will consolidate with OMA in September 19th, 2002, this work will subsequently continue within the OMA Location Working Group. This group will maintain and publish the protocols that can be used at the Le and Lr interfaces. Your references to these specifications will need to be updated, details will be available after November 15th in an LS from OMA.

It is our intention to report the progress of the work on the Lr interface at each 3GPP TSG CN and SA plenary.

To GSMA Serg
Action: LiF-SIG Roaming ah kindly asks GSMA SerG to note SIG's decision

To TSG SA2:
Action: Please review attached TR and provide comments to this LS.

We would like to highlight the following issues related to the transfer of privacy related information like, pseudo-ID's, codewords, Etc.

Please review the TR and decide if it can be used as input for 23.271

To CN4:
Action: LiFSIG Roaming ah kindly asks CN4 to note LiF's response to SA2 and LiF SIG Roaming work will continue in OMA to comply CN4 decision.

To TSG SA3:
Action: LiF SIG Roaming ah LiF-SIG Roaming kindly asks TSG SA3 to provide recommendations for an acceptable security protocol.

Note: Liaisons to this document need to be addressed to OMA Location working group.
Please be advised that the next OMA Location workgroup will meet November 11th till 15th.

LIF DELIVERABLE COPYRIGHT NOTICE AND DISCLAIMER

LIF Privacy Guidelines

Contents

1 Revision History 3
2 Introduction 4
3 Definitions 5
4 Privacy principles for location data 6
5 Right to control location data disclosure and usage 7
6 Conceptual architecture 9
7 Disclosure of location data 11
8 Location data usage after disclosure 13
9 Appendix A: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 14
10 Appendix B: Privacy Laws 16
11 Appendix C: Use cases 20

1 Revision History

0.1	28-Aug-2001	Kari Oinonen, Nokia	Proposal for Privacy AHG in LIF#4 meeting
0.2	17-Sep-2001	Kari Oinonen, Nokia	Updated
0.3	24-Oct-2001	Kari Oinonen, Nokia	Updated
0.4	7-Nov-2001	Kari Oinonen, Nokia	Updated
0.5	7-Dec-2001	Kari Oinonen, Nokia	Updated after LIF#5 meeting
0.1.0	16-Jan-2002	Kari Oinonen, Nokia	Updated
0.2.0	1-Mar-2002	Kari Oinonen, Nokia	Updated after LIF#6 meeting
0.3.0	15-Mar-2002	Kari Oinonen, Nokia	Updated
0.4.0	25-Mar-2002	Kari Oinonen, Nokia	Updated
0.5.0	8-Apr-2002	Kari Oinonen, Nokia	Updated
0.6.0	22-Apr-2002	Kari Oinonen, Nokia	Updated
0.7.0	20-Jun-2002	Kari Oinonen, Nokia	Updated after LIF#7 meeting
0.8.0	17-Sep-2002	Kari Oinonen, Nokia	Updated in LIF#8 meeting
2.0.0	19-Sep-2002	Kari Oinonen, Nokia	Final version (public release)

Contributors

Robert Beeson, Lucent
Fredric Bonnard, Alternis
Linus Claesson, Ericsson
Victoria Gray, ETSI
Wayne Hulls, Hutchison 3G
Anette Järn, Telia
Shah Karim, Motorola
Andres Kull, Elvior
Yasser M. Nafei, Motorola
Carl Reed, Open GIS

2 Introduction

Knowledge of location opens the possibility for providing highly personalised services and applications. At the same time, the improper or unauthorized use of location can be a threat to individual privacy. Privacy management of location data should therefore be given particular attention. Open access to the location of a consumer represents a threat to the privacy of that consumer as their location may be of utmost intimacy, especially when consumer location is combined with consumer identity or other accumulated profile information. For example, the tracking of someone's whereabouts can be used to provide significant insight into an individual's habits, preferences, and personal life. Knowledge of location behaviour gives marketers, sales organisations, hucksters, tricksters and outright criminals an opportunity to benefit on, or directly harm the consumer of location based services. On the other hand, location data provides rich contextual information that enables service providers to deliver highly personalised services that better address and provide for the anticipated needs of a consumer. Due to the concern of consumers as well as both existing and forthcoming legislation, there is an urgent requirement to provide consumers with control over the collection, use, and disclosure of their location information.

Objective and audience

This document is the guidelines of Location Interoperability Forum (LIF) for location data privacy. The target audience is application service providers, application developers, operators, terminal and network infrastructure manufacturers and other parties involved in the Mobile Location Service industry. The Guidelines are used in the LIF specification work and have been contributed to relevant standardisation bodies.

These guidelines are based on the fair information principles of the OECD, regulatory requirements, active or emerging, and expected demand from customers. The guidelines are intended to help anyone developing or providing Mobile Location Services to better comply with privacy.

Limitations

The LIF Privacy guidelines represent a recommendation, not a standard or regulation. Therefore, compliance to these guidelines is not mandatory for any party. Finally, this document is based on the best understanding of LIF member companies and does not necessarily cover all of the latest and local regulatory requirements. The reader should check local regulations and best practises before offering Mobile Location Service related products to customers.

3 Definitions

Aggregate data — Data that is separated from all personally identifiable information.

Consent — Agreement to collection and disclosure of location data under specified circumstances.

Controller — The person or juridical person who controls the privacy preferences. The Controller is normally the same as the Subscriber.

Informed consent — Consent that is given, with the opportunity of being informed of the consequence(s). Consent means permission to give location data to a requesting party in this document.

Location data — Geographical position of the target at a given time (lat/long/elevation or in another format)

LCS client — A location based service that requests location from a location service (LCS).

Personally identifiable information: Information that can be used to identify a physical or juridical person.

Requestor — The originating entity which has requested the location of the target.

Subscriber — A Subscriber is an entity (e.g. a user or juridical person) that is engaged in a Subscription with a service provider. (The subscriber pays the bill of the subscription and may be e.g. the employer of the target.)

Subscription — A subscription describes the commercial relationship between the subscriber and the service provider.

Target — The entity being positioned. It can be a person, an animal or a vehicle, for example.

4 Privacy principles for location data

Principles for the handling of personal data were developed in the seventies as a reaction to the ability of computers to process registers of personal data fast and in an automated manner. The purpose of the early principles was to prevent the misuse of the technology. Fair Information Principles (FIP) for handling personal information have been formulated by many organisations. The OECD (Organisation for Economic Co-operation and Development) formulated its principles in 1980, and these are commonly accepted as a good baseline for proper handling of personal information. The relevant part is quoted in appendix i. For location based services these principles are directly applicable. It is strongly recommended to comply with the OECD FIP guideline. In addition it is also recommended to comply with the following principles. The intent is to sharpen the OECD principles specifically for location data.

1. **Collection limitation:** Location data shall only be collected when the location of the target is required to provide a certain service.

2. **Consent:** Before any location data collection can occur, the informed consent of the controller has to be obtained. Consent may be restricted in several ways, to a single transaction, certain service providers etc. The controller must be able to access and change his or her preferences. It must be possible at all times to withdraw all consents previously given, to opt-out with simple means, free of additional charges and independent of the technology used.

3. **Usage and disclosure:** The processing and disclosure of location data shall be limited to what consent is given for. Pseudonymity shall be used when the service in question does not need to know the identity being served.

4. **Security safeguards:** Location data shall be erased when the requested service has been delivered or made (under given consent) aggregate.

From this it should be clear that the LIF recommendation is to offer location services in such a way that the controller must be able to give his/her informed consent for collection and disclosure of location data. This consent is referred to as the opt-in principle in this document, in contrast to the opt-out principle, where the controller actively must decline location data from being shared with others.

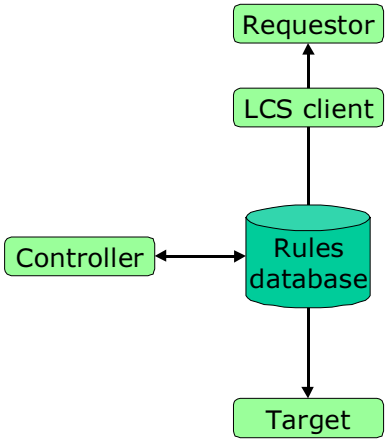
Lawful access to location information

With the authority of law all the mentioned privacy principles may be overruled. The two common cases are emergency calls and lawful intercept. The most common overriding of location privacy is emergency calls. The emergency service provider must be able to retrieve the location of the caller by law in many countries and this is irrespective of any privacy preferences.

5 Right to control location data disclosure and usage

The cellular subscriber or the mobile terminal user has the right to approve or deny collection and disclosure of location data.

The terminal user and the subscriber is not always the same person. For example, the employer who controls the privacy preferences can position an employee that uses a terminal at work. To be clear in terminology a ***controller*** is the one that decides on the privacy preferences to be followed by a location service. A ***target*** is the individual using the terminal, the one that is being positioned. Normally, the controller is also the ***subscriber*** of the target terminal and the privacy rules may be part of the ***subscription.*** The ***requestor*** is the party that initiates a service request finally leading to the positioning. **LCS client** presents the actual positioning request to the location service. The controller can authorize another party to configure the privacy preferences. In practice transferring this right may happen in several possible ways. Two common cases are presented below as examples.



Employer and employees

When an employer wants to track the location of his employees by tracking their mobile terminals, the consent of each employee must be acquired separately. This can happen at the time of signing a contract of employment, by clearly stating that by signing the contract the employee agrees to be tracked geographically by the employer. Alternatively a separate contract about tracking can be signed.

The responsibility of acquiring employee consent must also be agreed between the employer and the party providing the location service, like the cellular operator. If the employer is responsible, the operator must have an agreement with the employer removing the responsibility from the operator. On the other hand, if the operator is responsible, there must be an agreement guaranteeing that the employer respects the rules agreed between operator and employee.

Regardless of the means of acquiring an employee's consent the employee must know beforehand that he may be tracked, or otherwise his consent must be asked for separately when the need for tracking arises. It should also be noted that in practice the employee either agrees that he configures his privacy preferences himself so that his employer may track him, or he gives the right to configure his privacy preferences to his employer.

Parents and children

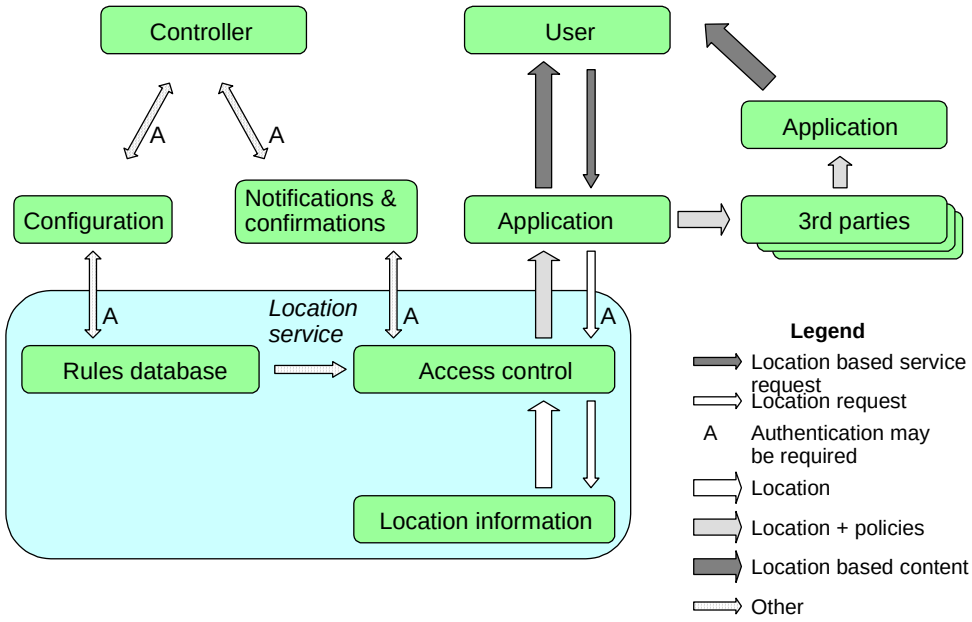
When parents want to track the location of their child the situation may be different than in the employer-employee case. By law, a child is a minor and has parents or legal guardian(s). The questions which arise are: May parent(s) or guardian(s) decide on the right of a child's privacy and can they track a child's location even without her/his knowledge and/or consent. The recommendation is that the parent is the controller. Although tracking might be allowed from a legal point of view, the LIF recommendation is to at least notify the child when he is positioned or to be tracked geographically.

6 Conceptual architecture

The figure below illustrates the conceptual architecture that supports mobile location services privacy. The basic principle is that location data is disclosed to an application (or service) by a location service. A location service consists of a location data entity, which already has the location data or uses a positioning method for location determination, a location access control function and access control rules database.

In the access control the application is first authenticated. Various technologies can be used for the authentication, like username and password or certificates. Following successful authentication the application is authorized in one of the ways described in the 'Disclosure of location data' chapter below. The authorization then enables access to certain kinds of location data.

When location data is delivered to the application, it must be done securely. This means that confidentiality and integrity of the data are preserved. A non-repudiation principle must also be applied due to possible privacy violations. Non-repudiation can be achieved through a trusted log, for example, which proves that a certain party has been given certain location data.



In practice the controller presented in the figure is usually the same as the target. A user of a location service is also often the target.

After location data is delivered to the application, the issue is how the location data is used and how it is passed on to third parties. This is discussed in chapter 7. The life span of location data is thus divided into two major parts; before and after disclosure to the application. The first part is taken care of by using technology such as authentication and authorization and supported by privacy policies, and the second part is enforced mainly through policies.

There are several possible means as to how the controlling function can be implemented. It can be over a browsing interface (http, WAP, etc.) for configuration towards a remote server. It can be IVR (interactive voice response), SMS or IN (intelligent network a la Camel) services. If configuration, notification and confirmation are not inside the same trusted domain as the location service, authentication is needed. It should be possible to handle the controlling function via the terminal.

Controlling function can also be implemented so that controller gives authorization tokens to an application. In practise this means that some service, or the terminal the controller is using, does it in behalf of the controller. These tokens can be digitally signed documents or just a codeword, and they authorize the application to get information from a location service. So, instead of configuring consent to give location to a certain application in the rules database, the controller may allow the application to carry his consent to the location service (where it can be added to the rules database if it is more than one time consent).

This conceptual architecture has no opinion on the technical realisation. It can be in a single server or a mobile terminal. What is indicated as one function can be divided into several parts given that all the parts are trusted or several functions can be bundled into a single function. In practice this means that part of the total privacy can also be implemented in the location based service client or another entity outside the location service itself. See the use cases chapter for examples of this.

7 Disclosure of location data

The basic principle for disclosing location data is confirmed opt-in, which means that the controller must give his/her informed consent for collection and disclosure of location data. The controller shall know the purpose of the collection and to whom it is disclosed for the opt-in to be informed.

A target terminal offers two other functions related to privacy in addition to the access to an application: notification with or without confirmation. Notification informs the target about ongoing positioning and confirmation means asking permission for positioning. The use of notification and confirmation is a part of the rules database configuration.

Reasonable security safeguards shall protect a disclosure according to FIP. To achieve this authentication of the LCS client and encryption of the data will usually be required. If the application is inside a trusted domain, such as operator premises, and only trusted parties can use it, authentication is not mandatory.

It is important that all the third parties to whom the location data is disclosed know how it may be used. Therefore the policies agreed between the location service and the controller party must be disclosed together with the location data.

There are two ways of getting the controllers informed consent for collection and disclosure of location data:

1. **Permission asked.** The authenticated identity of the requesting party is presented in an understandable form to the controller. Additional information like the planned usage, policy on storage and forwarding to third parties and if pseudonymity is offered may also be given. The now informed controller decides whether location data may be collected and disclosed in this specific case. The controller may optionally give permission for a longer period or even permanently.

2. **Predefined permission.** The controller has beforehand given informed consent for one or several location services. Special care should be taken with written or electronic subscriber agreements where privacy preferences are given together with other service subscriptions. Changing of user preferences must be easy and free of any additional charges.

The consent can be directly stored into the rules database of a location service, or it can be an authorization token given to an application like described in chapter 6. The authorization token can even be stored at the application, and it is then presented to the location service later.

The controller may accept disclosure of location data under pseudonymity. An identity service translates from target MSISDN (or whatever is used) to a temporary pseudo identity which is given to an application for referring a target in a location request.This way the target's real identity remains unknown for the application. If the same temporary identity is used over several requests, the anonymous identity becomes a permanent pseudonym. This could happen through one time or predefined permission and in both cases pseudonymity is recommended. Typically pseudonymity would be used when requestor is same as target, in other words the target itself is using the application.

Personally identifiable information should only be made available to service providers when it is required to provide the value added services. Special care should be taken in order that anonymous location data cannot be connected to an individual because other unnecessary information was included. The disclosed location shall not be more accurate than necessary for the service (country, city, street). Any location data should not be stored except where necessary for the provision of the service and subject to user's informed, unambiguous consent. (i.e. there should not be any sort of 'log' of the location of a target).

When the location of a target can't be given to an application, it should also be remembered that possible error responses must not compromise target's privacy. If an error response, for example, says that location can't be given because the target mobile terminal is not powered on, it can already be considered as a privacy threat because it reveals something about target's current status.

The quality or type of disclosed location data can be modified or degraded before disclosure to improve privacy. For example, if accuracy is at a course-grained level, such as a city instead of a street, this might be an acceptable level of privacy for some users or use cases. The general rule is that the disclosed location data shall be of as low accuracy as possible for the particular application.

8 Location data usage after disclosure

Location data shall only be provided when a specified purpose of usage is given. An important issue is also whether location may be given to a third party, and under what conditions. The controller might also want to limit the length of time that the location data may by used by the other party. These preferences have either been configured by the controller and are delivered to the application together with the location data, or the application has presented a policy as to how to handle location data and the user has decided to accept that policy. Exchange of policies may happen as text documents, or in machine-readable form.

A key issue is that all the players in mobile location services value chain have the same understanding of privacy and practices that don't leave any holes. If disclosure procedure, for example, is handled properly, but location data ends up in the hands of a third party, which does not respect the agreement on policies, privacy is lost. Privacy requires chain of trust, which is based on agreements. The trust chain begins from the target terminal, goes through an operator and service platform, and through one or more service providers.

9 Appendix A: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

This is an extract from the full OECD Guideline that can be found on the website: http://www.oecd.org/oecd/pages/home/displaygeneral/0,3380,EN-document-43-1-no-24-10255-43,FF.html

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) With the consent of the data subject; or

b) By the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:

a) To obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) To have communicated to him;
Data relating to him;
Within a reasonable time;
At a charge, if any, that is not excessive;
In a reasonable manner; and in a form that is readily intelligible to him;

c) To be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) To challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures that give effect to the principles stated above.

10 Appendix B: Privacy Laws

EU

In 1995 and 1997, the EU enacted two directives in order to harmonize data protection laws throughout the EU, to ensure citizens' adequate levels of privacy protection and to allow free flow of personal information throughout the member states. In July 2000, an additional proposal was issued to provide further privacy protection in the electronic communications sector.

The Data Protection Directive from 1995 sets the benchmark for the processing of personal information in electronic and manual files and the movement of such data.

The Telecommunications Directive from 1997 sets the benchmark for privacy protection in telephone, digital television, mobile networks and other telecommunications systems. It provides additional privacy protection to EU citizens by imposing obligations on carriers and services providers. The directive sets restrictions on access to billing information and marketing activities, and it gives consumers the option to block their phone numbers. Additionally the directive requires carriers and service providers to delete information related to a call once the service is completed.

"The Directive on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector", issued in July 2000 replaces the Telecommunications directive and further strengthens privacy protection in the EU once implemented in national legislations. The directive provides a broader perspective of electronic communications and it ensures protection of all information transmitted across different electronic communications media, prohibits unsolicited e-mail without opt-in consent, and protects mobile phone users from location tracking and surveillance.

All EU member states are required to enact implementing legislation that follows the EU directives and provide independent bodies (a data protection commissioner or agency) to ensure the enforcement of the rules.

The directives impose an obligation on member states to ensure that personal information relating to EU citizens has the same level of protection when the information is exported and processed in countries outside the EU. This requirement has resulted in a growing pressure in many countries outside the EU, including the U.S., to enact stronger privacy protection laws.

US

Constitutional right to privacy is provided by the Fourth Amendment's protection against unreasonable search and seizure. The U.S. has no comprehensive privacy protection law for the private sector and no independent privacy oversight agency. Instead, self-regulation and sectoral laws have been adapted to protect consumers' privacy.

The best known of the federal laws is the Children's Online Privacy Protection Act, which went into effect in May 2000. The Act applies to commercial web sites that are directed to, or that knowingly collect information from, children under 13. With certain exceptions, these sites will have to obtain parental consent before collecting, using, or disclosing personal information from children. Under the Act, sites must give parents a choice as to whether their child's information can be disclosed to third parties, and give parents a chance to prevent further use or future collection of personal information from their child. Parents must also, upon request, be given access to the personal information collected from their child and a means of reviewing that information.

The Communications Act of 1934 (47 U.S.C., Section 222) states that carriers have duty of confidentiality to the customer, and that they can use customer proprietary network information (CPNI) only in provisioning services requested by the user. CPNI information cannot be used for any other purpose without the written authorization from the customer.

The Wireless Communications and Public Safety Act of 1999 further amends Section 222 of the communications act to protect consumer location privacy and states that carriers must have "express prior authorization" from customers in order to use CPNI information (including location data) for marketing purposes.

The Financial Services Modernization Act allows users to opt-out from the usage and sharing of their data for marketing purposes. The bill however permits banks, insurance agencies and stockbrokers to merge their databases, providing these organizations access to more detailed customer information than previously. Law previously prohibited affiliation of these businesses.

Negotiations between the U.S. and the EU on the "Safe Harbor Principles" started in 1995 when the EU threatened to cut off all data flows, which is essentially most record of business transactions between the continents, unless the U.S. could guarantee that EU citizens' privacy would remain protected in the hands of American companies.

EU commissioners suggested the U.S. Congress should adopt privacy laws similar to the EU directives, while U.S. officials promoted self-regulation, or industry codes that U.S. companies would follow on pain of punishment of the FTC. An agreement was reached in April 1998 and took effect in November 2000. The agreement set out the following rules: U.S. companies can write contracts with privacy commissioners in the EU that lay out how they will protect personal data entrusted to them, or they can follow the Safe Harbor Principles, modelled after the EU Directive privacy protection rules. Enforcement of the Safe Harbor rules would be carried out by private groups and backed by the FTC.

Canada

In Canada the Personal Information Protection and Electronic Documents Act of 2001 gives certain rights with respect to the collection, use or disclosure of personal information by federally regulated organizations. These include airlines, banks, telephone companies, cable television and broadcasting companies. The Act applies to personal information collected, used or disclosed in the course of commercial activities, whether in the "real" world or on the Internet. It also applies to personal information disclosed to another province or country for profit or gain, where the information is the subject of the transaction.

Australia

The Privacy Amendment (Private Sector) Act 2000 regulates the way the private sector organizations can collect, use, keep secure and disclose personal information. It gives individuals the right to know what information an organization holds about them and a right to correct that information if it is wrong. Consumers have the right to know *why* a private sector organization is collecting their personal information, *what* information it holds about them, how it will *use* the information and who else will *get* the information. Except for some special circumstances, consumers can ask to *see* this information and for the information to be *corrected* if it is wrong. Consumers can also make a *complaint* if they think their information is not being handled properly.

New Zealand

New Zealand is the only country outside of Europe with a comprehensive data privacy law, and it covers both government and business. New Zealand's law gives consumers access to their personal data, and it follows OECD guidelines. There are no data transport restrictions against countries with inadequate or no privacy policies. Instead New Zealand is trying to build an international environment toward compatible privacy policies among nations.

Japan

Japanese parliament appears poised to pass overarching legislation aimed at establishing a fundamental national privacy framework.

Latin America

Argentina is discussing about privacy with other members of the Mercosur South American trade pact, Brazil, Paraguay, and Uruguay, and with Internet groups in Chile, Bolivia, and Peru to develop a Latin American e-commerce framework.

Summary

Which laws to comply with, and what they mean in practice are of course the questions from operators, Mobile Location Services developers, and application service providers.

It is clear that a service operating in a certain country must obey the local laws. The problem with location-based services is that they are often global, meaning that they can be used in many countries. If the same service is to be used in multiple countries without doing country specific versions, the service should then operate according to the most strict privacy regulation. If the laws are contradictory, specific versions for different countries are needed, but fortunately the laws seem to be more like complementary.

If you want to be on the safe side, you should go according to EU directives. All the EU countries will adopt these, and privacy related directives are among the strictest ones in the world – so you most probably comply with local laws at the same time. This document is mostly based on the EU directives, so you should follow the guidelines given in chapters 2 – 6.

It should also be noted that implementing the more strict principles described in this document doesn't mean that the actual service in use must operate according to them, if local laws allow more relaxed interpretation. One practical example is the opt-in and opt-out principles. In EU opt-in is mandatory, and in US opt-out is often enough. For both principles, however, you need access control and rules database functionality introduced in chapter 4. The only difference is then that in US you can activate the service for a target without asking, and in EU you must ask first – same implementation serves both.

11 Appendix C: Use cases

In the following use cases privacy management functionality with some location-based services is demonstrated. For simplicity, no infrastructure needed for positioning is shown in the figures.

Term 'ID' means MS-ISDN, or some other identity. If pseudonymity towards a location-based service is supported, the ID is a pseudonym. 'LBS' means Location Based Service, and 'LS' Location Service.

The left side in the use case figures shows flow of events in physical elements, and right side the same flow in conceptual architecture.

Cases A and B show how the target controls privacy when the target himself is using network based services and network based location service.

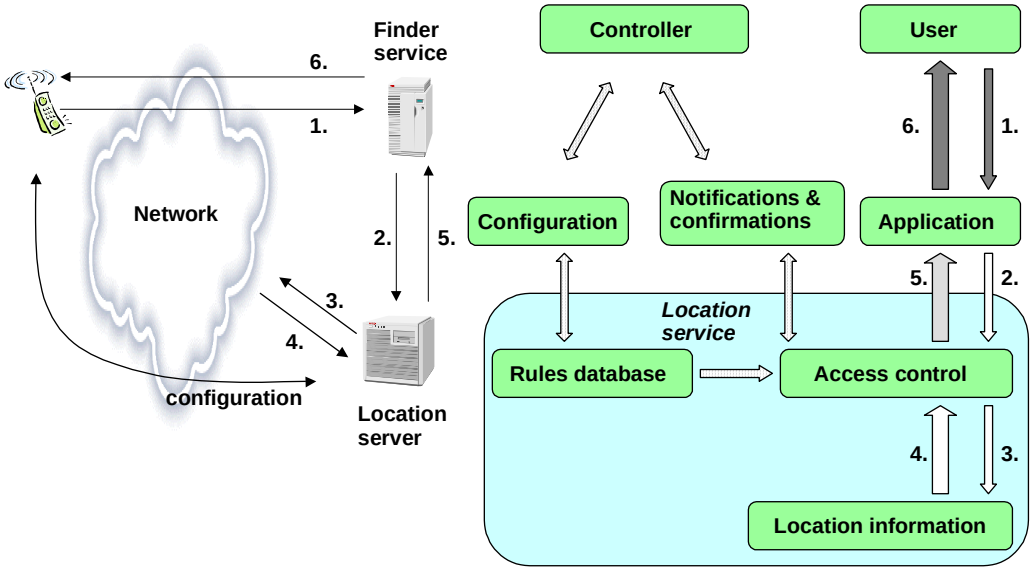
Case C shows how a person other than the target controls privacy.

Case D shows how the target controls privacy when a user of location-based services is another person.

Cased E and F show how part of privacy management can be outside of the location service.

Case G shows how privacy is managed by the target inside the target terminal when location is also available from the terminal.

A. LBS and LS in network



The target uses Finder service. Configuration of Finder service to rules database in the location server is done beforehand through browser, at the same time when the target subscribes Finder service (self provisioning). The browsing session is secure and the operator authenticates the target. When subscribing to the service, the target also checks what the policy is of Finder service for location data usage, and finds that acceptable. Therefore, no privacy confirmation from the target will be needed when the Finder service is used.

1. The target initiates a browsing session to Finder service, and asks for nearest restaurant. The target terminal also gives ID.

2. Finder service asks location from location server with the ID. Location server first authenticates Finder service and then checks if it is on the list of trusted services previously configured by the target to the rules database. Finder service is found from the list, so no separate confirmation from the target is required, and location request is forwarded in the location server for actual location determination.

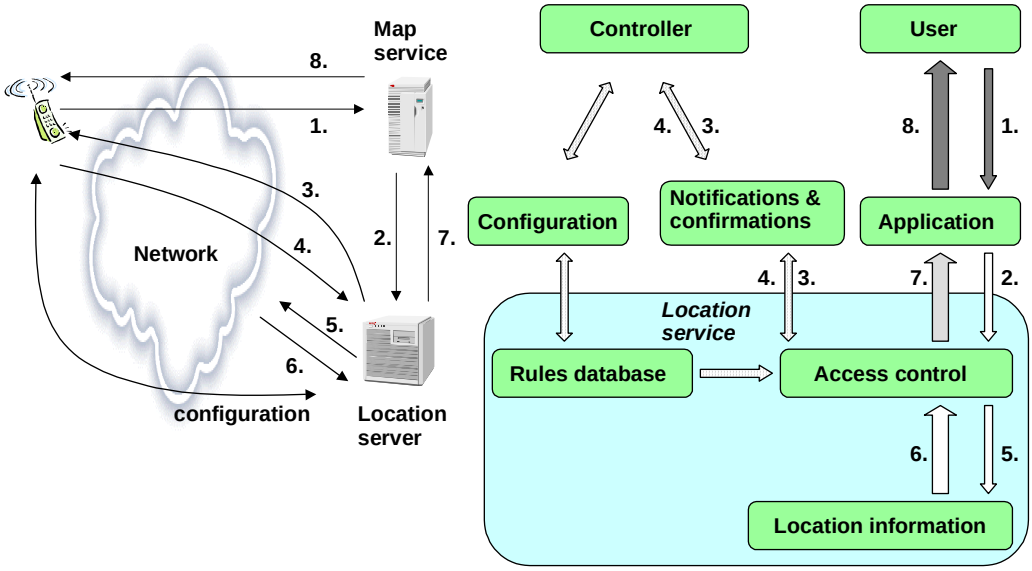
3. Location server sends positioning request to cellular network infrastructure.

4. The network sends positioning response to the location server.

5. Location server sends location response message to Finder service.

6. Finder service sends address of nearest restaurant to the target.

B. LBS and LS in network but privacy confirmation asked from the target



The target uses Map service. Difference to case A is that permission for positioning is asked from the target. Configuration of Map service to rules database in the location server has not been done beforehand, but instead the target has allowed that new location based services may be introduced to him by asking his confirmation for location usage. The target has, however, set a limitation: only those new services, which agree to use the location data only for providing a service the target himself is using, may be introduced. In practice setting this limitation is done by the target by accepting one of the few 'agreement templates' offered by an operator, and this can happen when subscribing for location service, or later through a separate browsing session where the target is authenticated before being allowed to change his preferences. From an operator point of view it means that when the operator has made an agreement with Map service, one of the agreement templates has been used. So, when the target invokes Map service for the first time, the operator can check whether the privacy policy of Map service matches the preferences of the target, based on the agreements between the operator and Map service, and between the operator and the target.

1. Target initiates a browsing session to Map service. Map service notices that this is a mobile terminal user, and therefore asks directly if the target wants a map of his current location, and the target answers yes. The target terminal also gives an ID.

2. Map service asks location from location server with the ID. Location server first authenticates Map service. Then it checks if Map service is on the list of trusted services previously configured by the target to the rules database, but Map service is not found there. Location server checks next if a request from Map service could be accepted based on other preferences of the target, and it turns out that this kind of service is allowed by the target but a separate confirmation is needed.

3. Location server sends a confirmation request to the target saying that Map service is asking for location data. This may happen through using the cellular supplementary services signalling standardized for this purpose, short message (SMS), WAP push, voice call or whatever method supported by the target terminal.

4. The target answers yes to the request and a response is sent to location server.

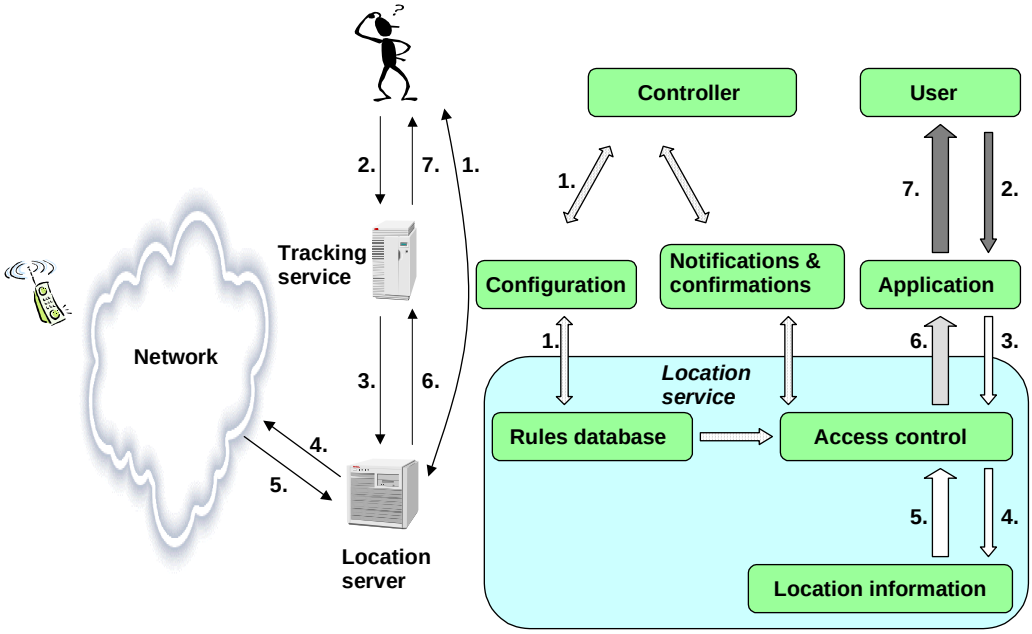
5. Location server sends positioning request to cellular network infrastructure.

6. The network sends positioning response to the location server.

7. Location server sends location response message to Map service.

8. Map service sends map of the target's current location to target.

C. LBS and LS in network, LBS not used by target



Target does not use a location-based service, but instead an employer tracks his employees.

1. Configuration of tracking service to rules database in the location server is done beforehand through browser, but by an employer instead of a target. The browsing session is secure and an operator authenticates the employer. In order to make this possible, the employer must have agreed with the operator that he has the right to do location privacy configuration for certain cellular subscriptions. In practise this can happen when the employer purchases some SIM cards, for example. At the same time when the operator gives the privacy configuration rights to the employer, the employer must agree that he is responsible of informing users of target terminals about tracking in a way required by local laws. This partially moves the liability of proper privacy protection from the operator to the employer.

2. Employer gets an urgent repair request of a broken device from one of his customers, and he wants to know where is his nearest service man in the field. The employer contacts Tracking service that already knows the IDs of the service personnel, and asks for the nearest man for a certain location.

3. Tracking service asks location of all the members of service personnel from location server. Location server first authenticates Tracking service and then checks if it is on the list of trusted services for each ID. Tracker service is found from all the lists, and no separate confirmation from any of the targets is required, and thus location requests are forwarded in the location server for actual location determination.

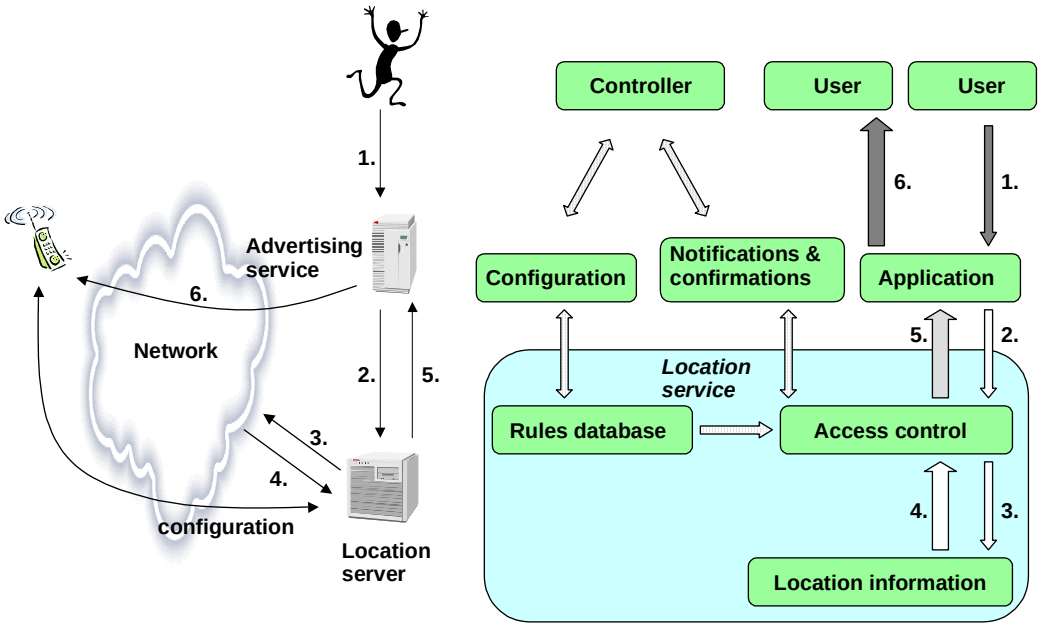
4. Location server sends positioning requests to cellular network infrastructure.

5. The network sends positioning responses to the location server.

6. Location server sends location response messages to tracking service.

7. Tracking service makes comparison and sends ID of nearest service man to the employer.

D. LBS and LS in network, LBS not used by target but target receives content



An advertiser uses location service, and target gets location based content. Configuration of Advertising service to rules database in the location server is done beforehand through browser, at the same time when the target subscribes to Advertising service (self provisioning). The browsing session is secure and an operator authenticates the target. When subscribing to the service, the target also checks what is the policy of Advertising service for location data usage, and finds that acceptable.

1. Advertiser sends a new advert to advertising service, together with definition of the area where the advert should be delivered to targets.

2. Advertising service sends a triggered location request to location server with the area defined by the advertiser as a parameter. Location server first authenticates Advertising service and then forwards the triggered location request in the location server.

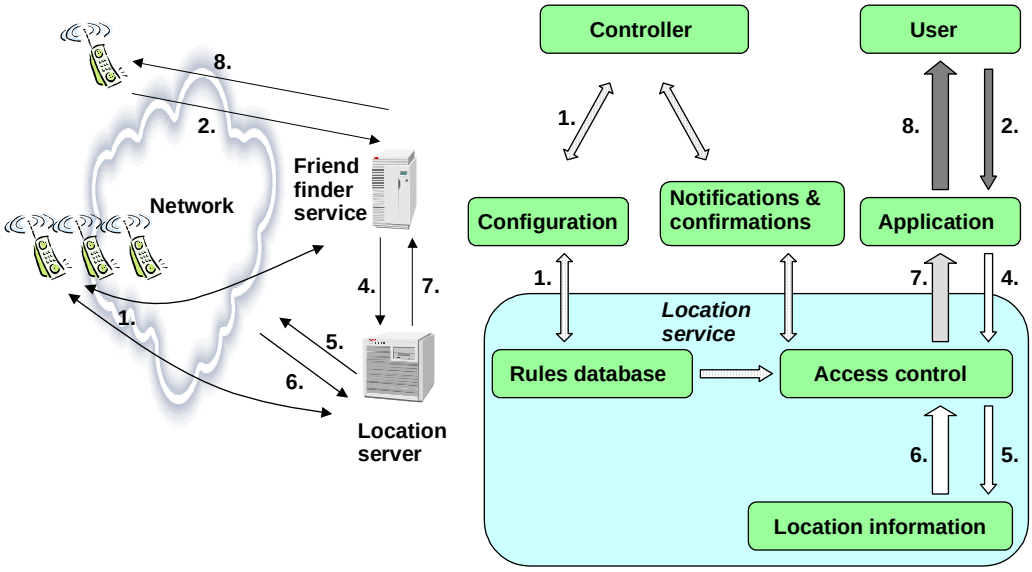
3. Location server sends positioning request to cellular network infrastructure.

4. The network sends positioning response with ID of target terminal to the location server when a target enters the defined area. The location server checks if the target has allowed giving location to Advertising service. Advertising service is found from the list in rules database, and also no separate confirmation from the target is required in the rules.

5. Location server sends location response message containing ID of the target to Advertising service.

6. Advertising service sends an advert to the target.

E. LBS and LS in network, privacy control in LBS



The target uses Friend finder service, and privacy is handled within that service instead of in a location service. In this case the primary rules database is in Friend finder service, and therefore the targets must make configurations there.

1. Each target defines his friends in the rules database of Friend finder service, and secure connection and authentication must be used when doing so. Each target must also configure to the location server rules database that Friend finder service is allowed to get his location. In practise configuration of the Friend finder service to the location server probably happens at the same time when subscribing to Friend finder, the target authorized Friend finder service provider to do it for him.

2. User goes through a browser to Friend finder service that authenticates him. User asks if any friends are near his current location, which is either given by the user or the user is positioned himself like described in use case A.

3. Friend finder presents a request for internal access control function to check who are the friends whose position the user is allowed to receive.

4. Location request is sent from Friend finder service to location server. Location server authenticates the request, and then checks that all the targets of the request have allowed the provision of their location to the Friend finder service.

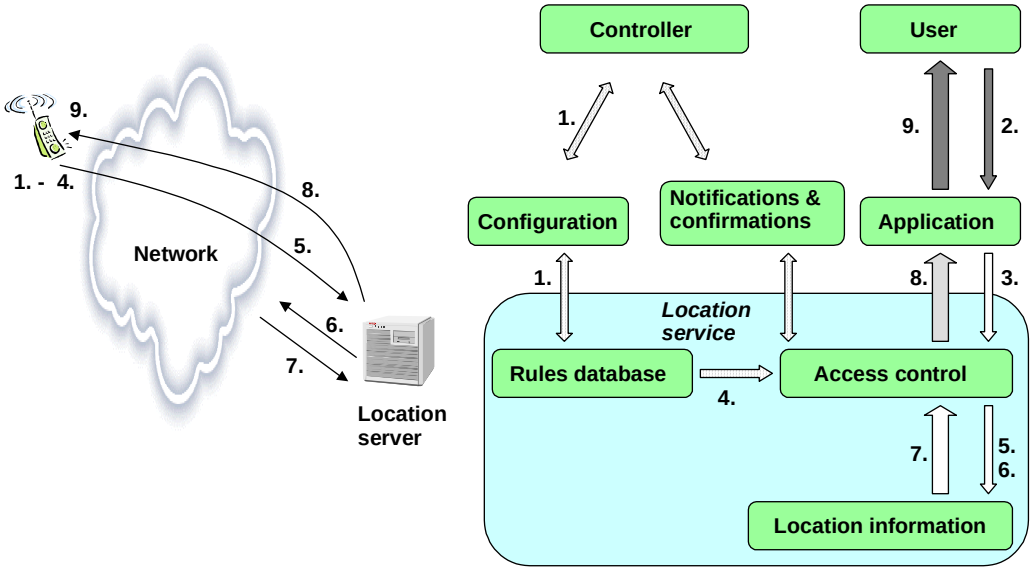
5. Location server sends positioning requests to cellular network infrastructure.

6. The network sends positioning responses to the location server.

7. Location server sends location response messages to Friend finder service.

8. Friend finder service makes comparison and sends ID of nearest friend to the user.

F. LBS in target, LS in network, privacy control in terminal



A terminal based navigation application is used. Location service is in network but privacy control is in terminal.

1. Target makes privacy configuration in terminal. Configuration means that those terminal based applications, which are allowed to get location from location interface of the terminal, are listed in the rules database. How the applications identify themselves is an application execution environment specific issue, meaning what kind of IDs should be on the list.

2. User initiates the Navigation application in the target terminal.

3. Navigation application asks location from a location interface in terminal and presents also some kind of application ID.

4. Access control function checks if the application is on the list of trusted applications in the rules database, and finds it there.

5. Location request is sent from target terminal to location server. Location server authenticates the request meaning that it makes sure that the request comes from the identified terminal, and then checks that the target has allowed giving its own location to itself. Therefore, the location server has the same kind of privacy control functionality as shown in use cases A-D, but it is not presented in this figure.

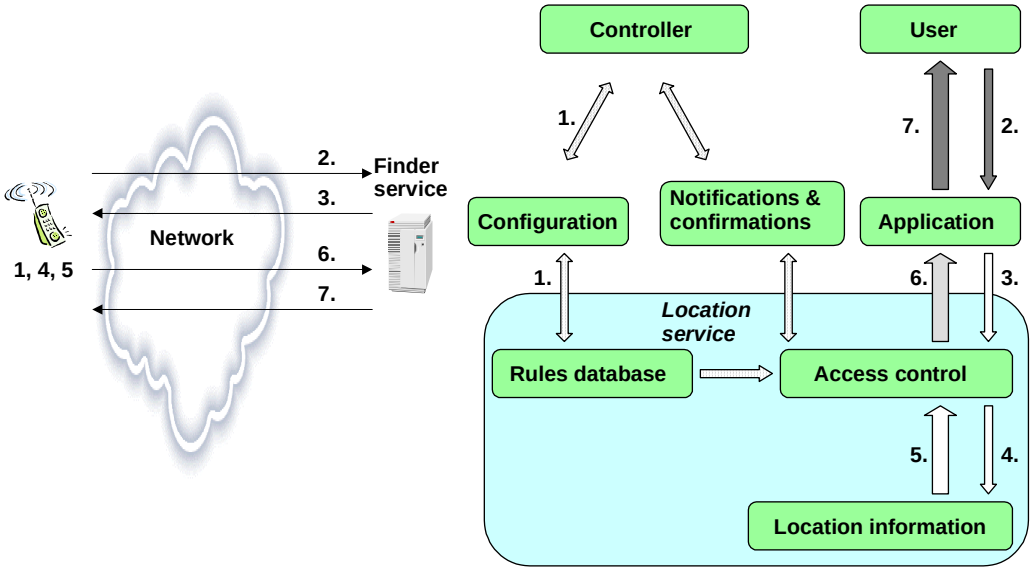
6. Location server sends positioning request to cellular network infrastructure.

7. The network sends positioning response to the location server.

8. Location server sends location response message to the target terminal. In the terminal the access control function makes sure that location goes to right application.

9. Navigation application presents navigation advice to user.

G. LBS in network, LS in terminal



Target uses Finder service, but difference to case A is that location service is in the terminal.

1. Configuration of Finder service to rules database in the target is done beforehand. This can be done manually, or assisted by Finder service provider, for example. Target user also checks privacy policy of Finder service, finds that acceptable, and defines that no separate confirmation is needed when location is requested by the Finder service.

2. Target initiates a browsing session to Finder service, and asks for nearest restaurant.

3. Finder service asks location from the target. Target first authenticates Finder service and then checks if it is on the list of trusted services in the rules database of target terminal. Finder service is found from the list, and location request is forwarded to location interface of the target terminal for actual location determination.

4. Positioning request is given to some terminal based positioning entity.

5. The positioning entity gives response to location interface of the target terminal.

6. Location interface sends location response message to Finder service.

7. Finder service sends address of nearest restaurant to target.