

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: May 15, 2011

W. Haddad  
Ericsson  
E. Nordmark  
Oracle  
November 11, 2010

Privacy Aspects Terminology  
draft-haddad-alien-privacy-terminology-06

## Abstract

This memo introduces terminology for the main privacy aspects. The prime goal is to avoid situations where different interpretations of the same key privacy aspects result in different requirements when designing specific solutions, thus leading to an unnecessary confusion.

## Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 15, 2011.

## Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as

Internet-Draft

Privacy Terminology

November 2010

described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Conventions used in this document . . . . .	<a href="#">4</a>
<a href="#">3.</a>	General Terminology . . . . .	<a href="#">5</a>
<a href="#">4.</a>	Privacy . . . . .	<a href="#">6</a>
<a href="#">5.</a>	Overview of Different Privacy Aspects . . . . .	<a href="#">7</a>
<a href="#">5.1.</a>	Anonymity . . . . .	<a href="#">7</a>
<a href="#">5.2.</a>	Unlinkability . . . . .	<a href="#">7</a>
<a href="#">5.3.</a>	Relation Between Anonymity and Unlinkability . . . . .	<a href="#">8</a>
<a href="#">5.4.</a>	Undetectability and Unobservability . . . . .	<a href="#">8</a>
<a href="#">5.5.</a>	Pseudonymity . . . . .	<a href="#">9</a>
<a href="#">5.6.</a>	Location Privacy . . . . .	<a href="#">9</a>
<a href="#">6.</a>	Security Considerations . . . . .	<a href="#">10</a>
<a href="#">7.</a>	Informative References . . . . .	<a href="#">11</a>
	Authors' Addresses . . . . .	<a href="#">12</a>

Internet-Draft

Privacy Terminology

November 2010

## 1. Introduction

Privacy is becoming a key requirement to allow deployment of specific internet services. However, privacy has many aspects, which differ in scope, properties and limitations.

To avoid any possible confusion in ongoing and future works with regard to the meanings of privacy in some particular scenarios, and to differentiate between requirements related to each scenario, privacy aspects have to be well defined before designing any solution. It is the intention of this memo to introduce terminology for the main aspects of privacy.

## 2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[TERM](#)].

### [3.](#) General Terminology

#### Item of Interest (IOI)

An Item of Interest (IOI) represents what an attacker is trying to discover, learn, trace and possibly link to other IOI(s), in order to identify its target. Examples of IOI include a subject, event, action (e.g., send, receive, move, etc), specific type of messages, etc.

#### Knowledge

In the field of privacy, knowledge refers to the information available to an attacker about its target. In terms of IOI, knowledge can be described by the probability of one or more IOIs. Consequently, more knowledge means more accurate probabilities. We refer to any prior information available to an attacker about a specific target as background knowledge.

#### Pseudonym

A pseudonym is an identifier of a subject (e.g., user) to a

particular transaction, which is different than any of the user's real names. This means that in the normal course of events, a pseudonym is not sufficient to associate the transaction to a particular subject.

## Digital Pseudonym

A digital pseudonym is a unique identifier (at least with very high probability) suitable to be used to authenticate the holder's IOIs relatively to his/her digital pseudonym, e.g., to authenticate his/her messages sent.

Another utility example is to set up an online account with an organization without revealing personal information, e.g., a public key.

Note that using digital pseudonyms, accountability can be realized with respect to pseudonyms.

## [4.](#) Privacy

Privacy is a fundamental human right. The most common definition of privacy is the one by Alan Westin: "Privacy is the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others".

Privacy is a general term that involves several different aspects. These aspects enable features like hiding the node's address(es) (e.g., MAC and/or IP), name(s) (e.g., DNS), and/or location(s), in addition to hiding specific IOIs. One or more of these features can be obtained during one particular session.

In wireless telecommunications, privacy addresses especially the

protection of the content as well as the context (e.g., time, location, type of service, ...) of a communication event.

Consequently, neither the mobile node nor its system software shall support the creation of user-related usage profiles. Such profiles basically comprise of a correlation of time and location of the node's use, as well as the type and details of the transaction performed.

The main privacy aspects are anonymity, unlinkability, undetectability, unobservability, and pseudonymity. Note that one way to achieve privacy is by disconnectivity, i.e., not being connected to a network.

## [5.](#) Overview of Different Privacy Aspects

As mentioned above, privacy is a general term, which refers to many different aspects. In the following, we define the main privacy aspects and describe the different relations between them.

### [5.1.](#) Anonymity

Anonymity is the state of being not identifiable within a set of subjects (e.g., node, user) called anonymity set. The sender(s) anonymity set(s) can be the same as the recipient(s) anonymity set(s) or they can overlap or simply be disjoint. But it should be noted that a set of possible subjects depends only on the knowledge of the attacker and may vary overtime. However, as the attacker's knowledge is expected to only increase in most applications, this means that the anonymity set can only decrease. Consequently, anonymity is the stronger, the larger the respective anonymity set is. Following the above description, it becomes clear that the anonymity concept is very much context dependent.

In the security field, anonymity is a property of network security. An entity "A" in a set has anonymity if no other entity can identify "A", nor is there any link back to "A" that can be used, nor any way to verify that any two anonymous act are performed by "A".

From a user perspective, anonymity ensures that a user may use a resource or service without disclosing the user's identity.

In wireless networks, anonymity means that neither the mobile node nor its system shall by default expose any information that allows any conclusions on the owner or current use of the node.

Consequently, in scenarios where a device and/or network identifiers are used (e.g., MAC address, IP address), neither the communication partner nor any outside attacker should be able to disclose any possible link between the respective identifier and the user's identity.

## [5.2.](#) Unlinkability

Unlinkability of two or more IOIs means that from an attacker's perspective, these IOIs are no more and no less related after his observation than they are related with regards to his background knowledge.

For example, two messages (e.g., binding updates) are unlinkable for an attacker if the a-posteriori probability describing his background knowledge that these two messages are sent by the same sender and/or

received by the same recipient is the same as the probability imposed



by his a-priori knowledge (i.e., by observing the system).

From a user perspective, unlinkability ensures that a user may make multiple uses of resources or services without other being able to link these uses together.

### [5.3.](#) Relation Between Anonymity and Unlinkability

In terms of unlinkability, anonymity can be defined as the unlinkability of an IOI and any subject. For example, a sender anonymity means that a particular message is not linkable to any sender and that to a particular sender, no message is linkable. The same is true for recipient anonymity.

If we consider as an example, that the subject is a pseudonym, this means that the anonymity of a particular IOI can be defined as the unlinkability of the IOI to any pseudonym and an anonymous pseudonym is not linkable to any IOI.

A weaker property than the sender's anonymity and the recipient's anonymity is the "relationship anonymity" where two or more pseudonyms are unlinkable. This means that for senders and recipients, it is not possible to trace who is communicating with whom, though it may possible to trace who is the sender, or who is the recipient. In other words, sender's pseudonyms and recipient's pseudonyms are unlinkable.

### [5.4.](#) Undetectability and Unobservability

As described above, the anonymity and unlinkability states protect the relationship between an IOI and a subject(s) or other IOI(s). This means that in scenarios where anonymity and/or unlinkability are required, senders and recipients can still exchange unprotected IOI(s).

In contrast to anonymity and unlinkability, the undetectability of IOIs is the state that whether they exist or not is indistinguishable. In other words, undetectability protects IOIs from being exposed. That is, the message transmission is not discernable from a random noise. In addition, unlinkability does not mention any relationship between "could-be" IOIs and subjects causing them. Consequently, undetectability of an IOI cannot be achieved if the IOI is related to a subject(s).

On the other side, unobservability can be defined as the undetectability by unrelated subjects together with anonymity (even if an IOIs can be detected).

---

From a user perspective, unobservability ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.

### [5.5.](#) Pseudonymity

Pseudonymity is a weaker property related to anonymity as it means that one cannot identify an entity, but it may be possible to prove that two pseudonyms acts were performed by the same entity.

When digital pseudonyms are used, pseudonymity ensures that a user may use a resource or service without disclosing its user identity, but can still be accountable for that use.

For more literature about the privacy terminology content, please refer to [\[ANON\]](#), [\[ISO99\]](#), [\[PRIVNG\]](#), [\[FREEDOM\]](#) and [\[ANONP\]](#).

### [5.6.](#) Location Privacy

Location privacy is the ability to prevent other parties from learning one's current and/or past location. In order to get such ability, the concerned (i.e., targeted) node must conceal any relation between its location and the personal identifiable information.

In other words, when the location is considered an IOI, then location privacy means the unlinkability between a node's identity and its location.

In our context, location privacy refers normally to the topological location and not the geographic one. The latter is provided by other means (e.g., GPS) than an IPv6 address. But it should be noted that it may be possible sometimes to deduce the geographical location from the topological one.

## [6.](#) Security Considerations

This document introduces terminology for different privacy aspects. It does not raise any security issues.

## 7. Informative References

- [ANON] Pfizman, A. and M. Hansen, "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management - A consolidated Proposal for Terminology", Draft v0.31, February 2008.
- [ANONP] Schmidt, M., "Subscriptionless Mobile Networking: Anonymity and Privacy Aspects within Personal Area Networks", IEEE WCNC, 2002.
- [FREEDOM] Westin, A., "Privacy and Freedom", Atheneum Press, NY, USA, 1967.
- [ISO99] "ISO IS 15408", <http://www.commoncriteria.org/> , 1997.
- [PRIVNG] Escudero-Pascual, A., "Privacy in the Next Generation Internet", December 2002.
- [TERM] Bradner, S., "Key Words for Use in RFCs to Indicate Requirement Levels", [RFC 2119](https://www.rfc-editor.org/rfc/rfc2119), BCP , March 1997.

#### Authors' Addresses

Wassim Haddad  
Ericsson  
300 Holger Way  
San Jose, CA 95134  
USA

Phone: +1 646 2562030  
Email: [Wassim.Haddad@ericsson.com](mailto:Wassim.Haddad@ericsson.com)

Erik Nordmark  
Oracle  
17 Network Circle  
Menlo Park, CA 94025  
USA

Phone: +1 650 786 2921  
Email: [Erik.Nordmark@oracle.com](mailto:Erik.Nordmark@oracle.com)

