# ISO/IEC JTC 1/WG 7
# Working Group on Sensor Networks

| | |
|---|---|
| **Document Number:** | N053 |
| **Date:** | 2010-07-05 |
| **Replace:** | |
| **Document Type:** | Liaison Organization Contribution |
| **Document Title:** | Liaison Statement from JTC 1/SC 27/WG 5 to JTC 1/WG 7 on the ISO/IEC 3rd WD 29191 |
| **Document Source:** | JTC 1/SC 27/WG 5 |
| **Document Status:** | For consideration at the 2nd WG 7 meeting in US. |
| **Action ID:** | FYI |
| **Due Date:** | |
| **No. of Pages:** | 15 |

ISO/IEC JTC 1/WG 7 Convenor:

Dr. Yongjin Kim, Modacom Co., Ltd (Email: cap@modacom.co.kr)

ISO/IEC JTC 1/WG 7 Secretariat:

Ms. Jooran Lee, Korean Standards Association (Email: jooran@kisi.or.kr)

ISO/IEC JTC 1/SC 27 N8816

ISO/IEC JTC 1/SC 27/WG 5 N58816

REPLACES:N8277

**ISO/IEC JTC 1/SC 27**

**Information technology - Security techniques**

**Secretariat: DIN, Germany**

| | |
|---|---|
| **DOC TYPE:** | working document |
| **TITLE:** | **Text ISO/IEC 3rd WD 29191 -- Information technology -- Security techniques – Requirements on relatively anonymous unlinkable authentication** |
| **SOURCE:** | Project Editor (Kazue Sako) |
| **DATE :** | 2010-06-01 |
| **PROJECT:** | 29191 (1.27.81) |
| **STATUS:** | In accordance with resolution P1 (in SC27 N8828rev) of the 9th SC 27/WG 5 Plenary meeting held in Melaka, Malaysia (April 2010) this document is being circulated for **STUDY AND COMMENT**.<br>National Bodies and liaison organizations of SC 27 are requested to send their comments/contributions on the above-mentioned document by **2010-09-01.** |
| **PLEASE NOTE:** | For comments please use the SC 27 TEMPLATE separately attached to this document. |
| **ACTION:** | **COM** |
| **DUE DATE:** | **2010-09-01** |
| **DISTRIBUTION:** | P-, O- and L-Members<br>W. Fumy, SC 27 Chairman<br>M. De Soete, SC 27 Vice-Chair<br>E. Humphreys, K. Naemura, M. Bañón, M.-C. Kang, K. Rannenberg, WG-Conveners |
| **MEDIUM:** | |
| **NO. OF PAGES:** | 1 + 13 |

**** title change from "Requirements on relative anonymity with identity escrow" to "Requirements on relative anonymity unlinkable authentication" subject to SC 27/WG 5 approval***

ISO/IEC JTC 1/SC 27 N 8816

Date: 2010-06-1

ISO/IEC WD 29191.3

ISO/IEC JTC 1/SC 27/WG 5

Secretariat: DIN

# Information Technology — Security techniques — Requirements on relatively anonymous unlinkable authentication

*Élément introductif — Élément central — Élément complémentaire*

**Warning**

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard
Document subtype:
Document stage: (20) Preparatory
Document language: E

F:\krystyna\29191\N8816_3rdWD_29191_100601.doc STD Version 2.1c2

# Contents

Page

Foreword ........ iv

Introduction ........ v

1 Scope ........ 1

2 Normative references ........ 1

3 Terms and definitions ........ 1

4 General ........ 1

5 Framework ........ 2

6 Requirements ........ 3

Annex A (informative) ........ 5

# Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 29191 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

# Introduction

In Information Technology there is an ever increasing need to use cryptographic mechanisms for entity authentication and data authentication in order to prevent unauthorized access or to detect any manipulation of data. Previous work of art such as entity authentication and digital signatures succeed to provide means to protect system at the cost of revealing the identity of the entity being authenticated, or if not identity, a linkable information such as a pseudonym or a public key that is bound to the entity. It is therefore important to consider alternative framework that provides measures against unauthorized access without having the users to reveal their identity or linkable information. Yet fully anonymous authentication may cause different threat to the system. It is necessary to pursue a good balance between privacy and security. One approach is to authenticate a user that he/she belongs to an authorized group but his/her identity is revealed only to an escrow agent. Thus the user can enjoy privacy but he/she is not completely anonymous. Yet this authentication transaction is unlinkable, that is, if two transactions are performed, it is difficult to distinguish whether it is authentication of the same user in the group or two different users, unless the person who is trying to distinguish is the escrow agent. This document defines a model on partially anonymous unlinkable authentication and provides its requirements.

# Information Technology — Security techniques — Requirements on relatively anonymous unlinkable authentication

## 1 Scope

This document provides a model of relatively(partially) anonymous unlinkable authentication with identity escrow and defines its requirements. This document is aimed to provide guidance to the use of group signatures and relevant mechanisms for the purpose of data minimization and user convenience. It allows the users to control their anonymity within the group of registered users by choosing designated escrow agents.

## 2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

None.

## 3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

Partially anonymous authentication—method of verifying the user's access privilege where user's identity information is not revealed in course of verification but an escrow agent can reveal the identity information. '

unlinkable authentication – method of verifying the user's access privilege where one can not determine if two transactions are authenticating a same user or not.

escrow agent – authority who can identify the signer from the signed message. Note that an excrow agent may be appointed by the signer to each message the signer signs.

## 4 General

In the model of authentication and authorization of an entity, it has conventionally taken the following procedure: 1) identifying the entity, 2)authenticating that the entity is the claimed identity, and then 3) authorize the entity by checking if the identity belongs to an authorized group, perhaps using an access control list. This procedure successfully prevents unauthorized access. However, if forces the entity to reveal its identity. From the point of view of data minimization, it is desirable to provide a scheme of authentication and authorization where the entity does not provide its identity but prove that its identity belongs to the authorized group.

A sophisticated use of public key infrastructure allows user not to reveal his or her identity, by replacing the identity by a pseudonym or a public key. However this information can be used to link two authentication transactions and thus the user. That is, if two authentication transactions deal with a user with a same pseudonym, it means that the same user is being authenticated. If one transaction reveals say the address of the user, and the other reveals his or her telephone number, it results in linking the address and the telephone number of a user by matching the pseudonym. Therefore using linkable information may not be satisfactory solution from the privacy point of view.

Yet perfect anonymity within the group may not be suitable as the user has a potential of exploiting anonymity. Therefore this document provides a framework where users can enjoy unlinkable anonymity but to the escrow agent who can reveal the identity of the user when necessary. This framework is named a relatively anonymous unlinkable authentication. This document illustrates this framework and defines its security and privacy requirements.

# 5 Framework

In this framework, a typical scenario where a system grants access privilege equally according to the group a user belongs to is dealt. The group and access policy can be determined in either way: the users who are allowed to access form a group, or, a member of a certain group is always allowed to access. In the following, the system, or a verifier, wants to verify whether or not the user belongs to the group. The system does not necessarily learn who the user is. If that is necessary, the system can contact an escrow agent to identify the user.

In the framework of relatively anonymous unlinkable authentication, there are essentially four entities as described in Figure 1.

a) A membership issuer, or issuer for short, is an entity who registers members in the group by issuing members a group certificate.

b) A user is one who will be authenticated to a verifier.

c) A verifier is one who authenticates whether the user is within the group.

d) An escrow agent, or opener, is an entity who can identify the user from the authentication transaction.

Among above four entities, there are three basic operations in this framework.

- A process between a membership issuer and a user to perform group joining process. After this process a user obtains a certificate as a group member.

- A process between a user and a verifier to perform user authentication verifying whether the user is a group member or not.

- A process by an escrow agent to identify the user from the authentication transcript called the identification process.

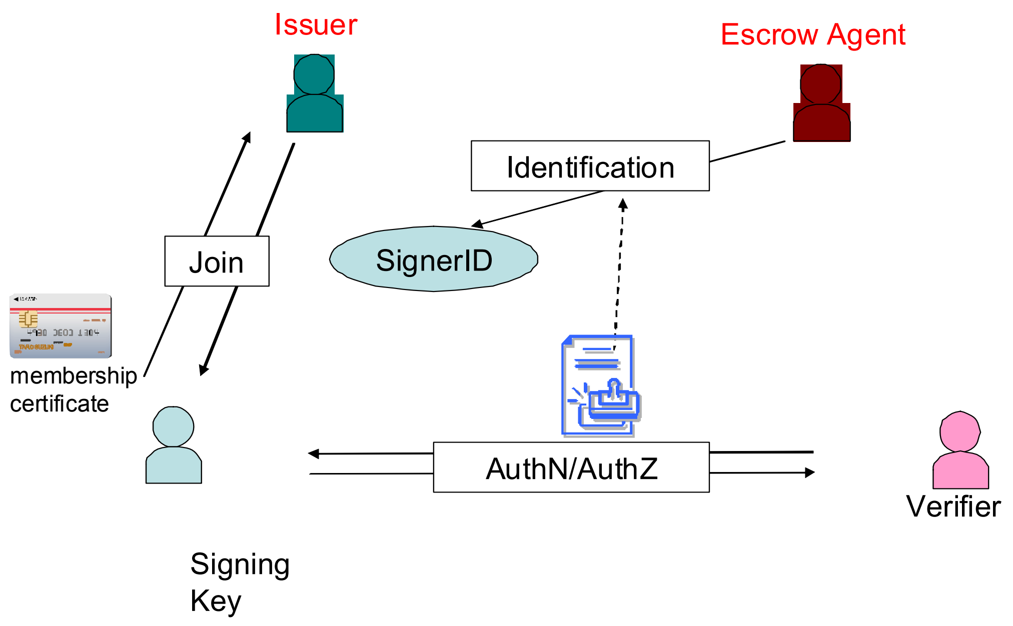

**Figure 1— Framework of relatively anonymous unlinkable authentication**

## 6 Requirements

The relative anonymity with identity escrow in the model of authentication and authorization should satisfy the following security and privacy requirements described below.

a) No one but the issuer shall be able to invite a new user to the privilege group.

b) If a verifier outputs accept at the authentication process, that means the user has a secret key received at the joining process with the issuer.

c) If a verifier outputs accepts at the authentication process, that means that the escrow agent can always correctly identify the user from the authentication transcript.

d) Through the authentication process, no matter how the verifier behaves, verifier can not obtain information about the identity of the user unless he or she colludes with escrow agent. This requirement infers unlinkable property, that the verifier can not obtain identity information of the user though linking two transactions.

e) An escrow agent cannot falsely claim identify of a user from the authentication transcript.

Bibliography

- Chaum and van Heyst: **“Group Signatures**.” EUROCRYPT 1991

- Kilian and Erez Petrank: “ **Identity Escrow**.” CRYPTO 1998

- Camenisch and Groth: “ Group Signatures: Better Efficiency and New Theoretical Aspects.” SCN 2004

- Furukawa and Imai: "**An Efficient Group Signature Scheme from Bilinear Maps."** ACISP 2005

- Isshiki, Mori, Sako, Teranishi and Yonezawa: " **Using group signatures for identity management and its implementation**." IDM 2006

# Annex A
# (informative)

## A. Usecases

In this section, some of the scenarios to use partially anonymous unlinkable authentication.

### A.1 Library usecase

In some countries, a care is taken regarding the list of the title of the books that one has borrowed from an library, as it may reflects his or her thoughts, conscience, and religion. However, part of such information is necessary when he or she does not return the book by due date. Framework of partially anonymous unlinkable authentication can be used in this scenario.

There will be a membership issuer, who will be issuing membership card for users. There will be users who wants to borrow a book form the library. There will be a librarian who checks if the user is a member of the library, and if the user is a member, performs the sign-out procedure of the book. There will be a head of the library, who plays the role of the escrow agent.

A user who comes to this library for the first time performs group joining process with a membership issuer, who may be a special librarian sitting at the registration desk. The user receives a certificate. When the user wants to borrow a book, then the user goes to the sign-out desk and performs user authentication that the user is a member of the group. Through the use of partially anonymous unlinkable authentication, the user remains anonymous within the group of registered members. The log entry would be the title of the book, the date of sign-out, and the due date to return the book, with a transcript that was generated through the authentication. The transcript does not reveal who borrowed that book. The transcript is unlinkable, that is, it is impossible to find from the log entries another book title that has been borrowed by the same user. However, if the user fails to return the book by the due date, then the head of the library may perform identification process of the borrower. The head of the library has a secret key which allows him to identify the borrower from the transcript. Then the head of the library may be able to send reminder notice to the borrower.

### A.2 Billing account usecase

Users have billing accounts such as bank accounts and credit card accounts. When shopping at a web store, it is important that the user has a legitimate billing account. However, there is a risk of conveying the exact account number to the web store, as it may be abused by the web store. On the other hand, there is a risk for the web store on receiving such exact account number of the customer, and the shop need to pay extra cost to keep these data secured from being breached. Framework of partially anonymous unlinkable authentication can be used in this scenario.

There will be a bank or credit card company, who will be issuing accounts to the users. There will be users who wants to buy goods a book form a web store. There will be a software at a web store who checks if the user is has a legitimate billing account, and if the user does have one, performs the selling procedure of the goods. The bank or the credit card company will play the role of the escrow agent.

A user when opening his bank account or credit card account performs group joining process with either a bank or credit card company. The user receives a certificate. When the user wants to buy some goods at the web store, the user engages user authentication at the web store and proves the user has a legitimate billing account at the claimed bank or the credit card company. Through the use of partially anonymous unlinkable authentication, the web store can verify that the user indeed has a legitimate account at the claimed organization, without learning the user's exact account number. The log entry would be the name of the goods, the date of purchase, the name of the bank or the credit card company that the user claimed to have account at, with a transcript that was generated through the authentication. The transcript does not reveal the exact account number. The transcript is unlinkable, that is, it is impossible to find from the log entries another goods that has been purchased by the same user. The web store passes this transcript to the claimed organization. The organization, the bank or credit card company, performs identification process on the transcript using its own key and successfully obtains the exact billing account. The user is comfortable that the web store does not learn his account number, and the web store is comfortable that it need not learn such private information.

## A.3 Passport usecase

Passports are usually the only way to identify oneself when travelling abroad. Besides the purpose of borderline control which is the original purpose of issuing passports, passports are used in civil procedures such as hotel check in and/or using credit cards at supermarkets. It is important to confirm that the user has a legitimate ID so that the user can be identified in case of a trouble. However, there is a risk of conveying the exact passport number to the hotel clerks and supermarket cashier, as it may be abused by them. On the other hand, there is a risk for the hotels and supermarkets on receiving the passport number of the customer, and they need to pay extra cost to keep these data secured from being breached. Framework of partially anonymous unlinkable authentication can be used in this scenario.

There will be a national authority, who will be issuing passports to the citizens. There will be users who travels the world. There will be a clerk at a hotel or a supermarket who checks if the user is has an authorized ID when providing service to them. The local embassy will play the role of the escrow agent.

A user when applying for passport performs group joining process with national authority. When the user is asked to show his or her ID at the hotel or supermarkets abroad, the user engages user authentication and proves the user has a legitimate passport issued by the claimed nation. Through the use of partially anonymous unlinkable authentication, the hotel or supermarkets can verify that the user indeed has a legitimate passport at the claimed nation, without learning the user’s exact passport number. The log entry would be the service they provided with the name of the country that the user claims to be from, with a transcript that was generated through the authentication. The transcript does not reveal the exact passport number. The transcript is unlinkable, that is, it is impossible to find from the log entries another services that has been provided to the same user. In case of troubles, the hotel or the supermarkets can present this trascript to the local embassy of the claimed country. The organization, the bank or credit card company, performs identification process on the transcript using its own key and successfully identifies the user. The user is comfortable that the civil organization does not learn his passport number, and the civil organizations are comfortable that they need not learn such private information.

## A.4 Intelligent Traffic System usecase

In order to improve traffic flow and provide the ability to do real-time analysis on intercity highway, frequent users of the route is issued a tag that can be read in a contactless manner and the use of the route is logged at an intelligent traffic control center. In order to protect the privacy of the users of the highway, the information captured should provide an appropriate level of anonymity to the users. In addition to the traffic analysis, the same tags are used for two other services. The first is tolling on a stretch of the highway and the second is to control the access to a car pool lane.

In the traffic analysis scenario, the car is either tracked anonymously to determine highway capacity utilization or it may be tracked in an pseudononymous fashion where a profile is built up over time of a vehicle’s use of the highway. For each car a list is created that includes the time of entry onto the highway, time of exit, place of entry and exit and days of use. This information is then used to do capacity planning based on actual usage patterns.

A vehicle is registered with a certificate authority and receives a tag. This tag is representative of the UID in the generic system ( Figure A2.) A second certificate is issued to be used in the traffic analysis process. This certificate is an example of the PID in the generic system (Figure A2) and called PID1 . Another certificate is requested and issued in the case that the vehicle forms part of a car pool (PID2).

When a vehicle that forms part of a carpool enters the highway, the tag is read by a reader and a request for access is made to access the car pool lane. The car pool proxy authenticated the PID2 against its allowed group database and issues an “authorized” or “denied” to the car pool lane monitor (service authenticator.) If the vehicle does not belong the car pool or its authorization to use the car pool lane is revoked, a request is made to the Disclosure Authority to provide the identity of the car owner for the issuing of a fine.

The traffic analysis system operates in two modes, the current, anonymous congestion mode where access to the highway is given and only the number of cars on a given section is noted. This is done in an anonymous fashion. When there are too many vehicles on the section of the highway, cars are denied access to the highway via traffic lights at the on-ramps. If the highway capacity is not filled, the cars are given access to the highway, but the access is logged with a temporary identification that expires when the car exits the highway. The temporary identification is an example of the AID in the generic system (Figure A2).

In this case, if it is picked up that the car is violating a traffic rule, access is again requested to the identity of the owner of the vehicle. The Anonymity/Identity Disclosure Authority is contacted for access to the identity of the owner of the vehicle and access is granted to the identity for the issue of a fine.

In the traffic analysis scenario, when a car that form part of the analysis project group  enters the highway through the request via the card reader at the on-ramp, the event is logged in a pseudononymous fashion where a profile is built up over time of a vehicle's use of the highway. For each car a list is created that includes the time of entry onto the highway, time of exit,  place of entry and exit and days of use. This information is then used to do capacity planning based on actual usage patterns. Again the identity of the owner is not available to the traffic analysis entity (Service Authenticator.) In a case of a traffic violation or emergency, the identity of the vehicle owner is obtained via the Pseudonymity/Identity Disclosure Authority and the traffic analysis dedicated proxy.

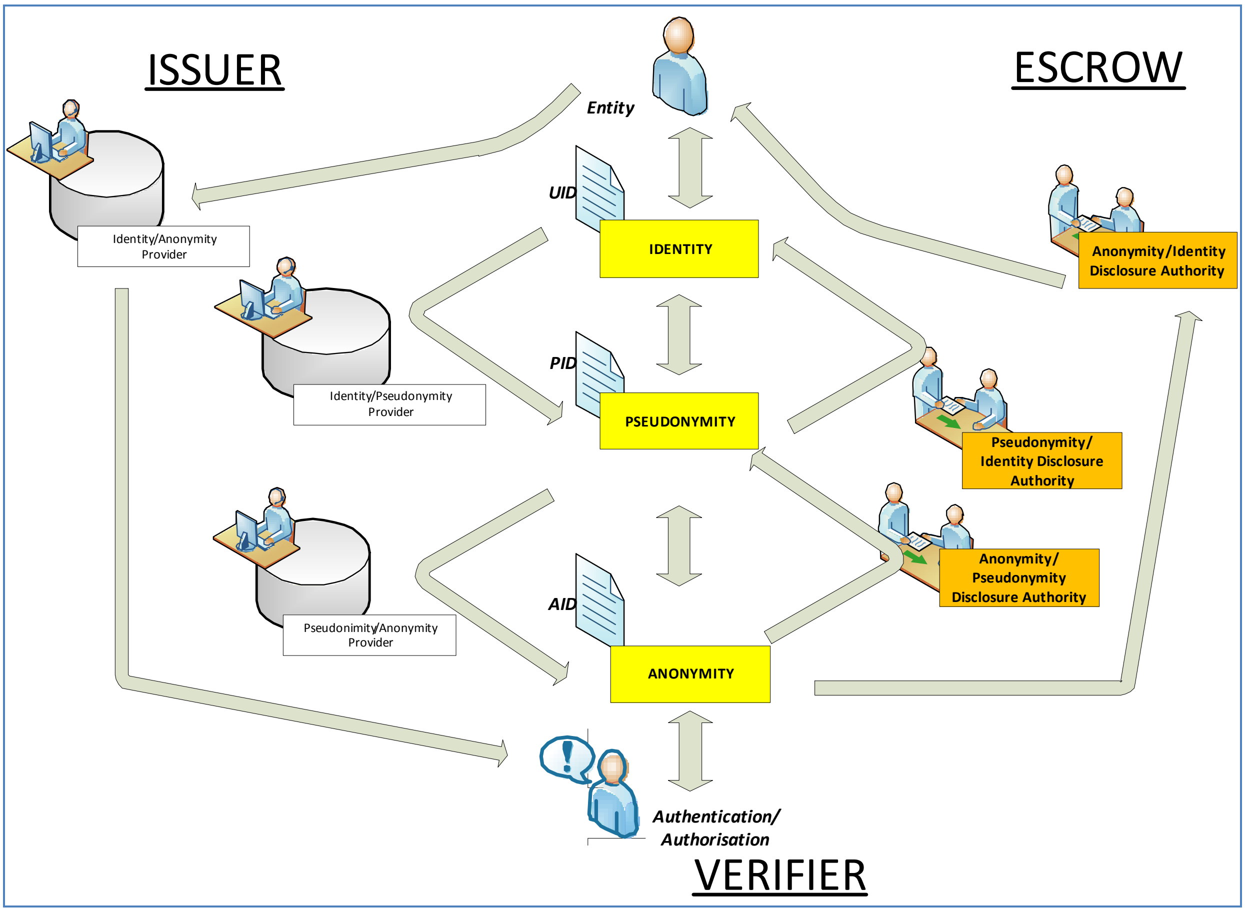
ISSUER
ESCROW
Entity
UID
IDENTITY
Identity/Anonymity Provider
Anonymity/Identity Disclosure Authority
PID
PSEUDONYMITY
Identity/Pseudonymity Provider
Pseudonymity/ Identity Disclosure Authority
Anonymity/ Pseudonymity Disclosure Authority
Pseudonimity/Anonymity Provider
AID
ANONYMITY
Authentication/ Authorisation
VERIFIER

**Figure A2 — Generic escrowed authentication system**