INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2009-2012

STUDY GROUP 17

Ref. TD 0640

English only

Original: English

Question(s):	10/17	Geneva, 16-25 September 2009

TEMPORARY DOCUMENT

Source: Editor of Rec. X.priva

Title: Draft Recommendation ITU-T X.priva, Criteria for assessing the level of protection for personally identifiable information in IdM

Draft Recommendation ITU-T X.priva

Criteria for assessing the level of protection for personally identifiable information in IdM

Summary

This Recommendation defines the criteria for assessing the level of protection for personally identifiable information (PII) of the identity provider and the relying party concerned in identity service, depending on the protection for personally identifiable information requested by them to the requesting/asserting party, and the type and use purpose of PII and maintain period of PII, as well as the technical and administrative measures for protection for PII.

Keywords

<Optional>

Introduction

<Optional – This clause should appear only if it contains information different from Scope and Summary>

1 Scope

This Recommendation defines the criteria for assessing the level of protection of personally identifiable information, including the ID information of the Requesting/Asserting Party issued from the Identity Provider.

The level of protection of the personally identifiable information of the Identity Provider can be assessed in terms of the technical and administrative factors or measures that the Identity Provider provides for the protection of the collected PII, and the appropriateness of the methods used to protect and manage the ID-related personally identifiable information during the process of ID

Contact:	Hyangjin Lee Korea Internet & Security Agency Korea (Republic of)	Tel: +82-2-405-5446 Fax: +82-2-405-5219 Email: jiinii@kisa.or.kr
Contact:	Inkyoung Jeun Korea Internet & Security Agency Korea (Republic of)	Tel: +82-2-405-5426 Fax: +82-2-405-5219 Email: ikjeun@kisa.or.kr

issuance and use.

To achieve this, this recommendation defines a level of protection for PII, and proposes general and common factors and an assessment methodology to assess this level.

The criteria defined in this recommendation target the Identity Provider only. Especially, this Recommendation is limited in application and service, managing the PII directly or indirectly, that is required form Relying/Asserting Party in order to issue an identity. In addition, the criteria have not to cut both ways, because business policy and requirements of the Identity Providers may be different from each others. Therefore, this Recommendation describes the general and common assessment criteria for the typical Identity Provider.

2 Reference

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 Identity [ITU-T X.idmreq]: Structured representations of an entity in the form of one or more credentials, identifiers, attributes, or patterns in a relevant context. Such representations can take any physical or electropitcal (digital or analog) form or syntax, and may have associated implicit or explicit time-stamp and location specifications.

3.1.2 Identity Provider [ITU-T X.idmreq]: An entity that creates, maintains, and manages trusted identity information for entities. An Identity Provider may include a Trusted Third Party, as well as Relying Parties and entities themselves in different contexts.

3.1.3 Requesting/Asserting Entity [ITU-T X.idmreq]: An Entity making an identity representation or claim to a relying party within some request context.

3.1.4 Relying Party [ITU-T X.idmreq]: An entity that relies on an identity representation or claim by a Requesting/Asserting entity within some request context

3.2 Terms defined in this Recommendation

3.2.1 Identity Life Cycle

[TBD]

4 Abbreviations and Acronyms

PII	Personally Identifiable Information
PPII	Protection for PII

5 Conventions

None

6 Threats of PII in IdM service

Editor Note: *Describe various threats of PII that may occur during managing and using PIIs, according to the Identity life cycle.*

[TBD]

7 Factors for assessing the level of protection for personally identifiable information

Editor Note: *Describe the common and general factors designed to assess whether proper measures are taken to protect the PII according to the Identity life cycle, based on threats of PII as described in Section 6.*

[TBD]

7.1 Infrastructure

This section proposes various items that are needed to protect PII, such as privacy policy, budget, staff education, etc. The assessment of the infrastructure for Protection for PII in Identity Provider determines whether or not these items are in place, through an evaluation of them.

7.1.1 Policy Infrastructure

Identity provider should have the budget and manpower that are above the certain level from the perspectives of the policy infrastructure, in order to protect the PII collected during the identity proofing process. The following table shows the factors that can be used to measure the protection level for PII from the viewpoint of the policy infrastructure.

Detailed Criteria	Description
The status of manpower	Checks whether the department in charge of protection for PII is available and the personal in charge of PII is assigned or not.
Scale of budget	Checks whether the budget is made to take political and technological actions for protection for PII or not.
The status of providing education and training	Checks whether training is provided to the personal in charge of PII.
The degree of appropriateness of the protection policy for PII	Checks whether the required guide is included in the protection policy for PII and updated periodically or not.
The responsibility of a PII controller	Checks whether a person has a clear responsibility to guarantee fair processing in respect of the data subject, determines the purposes and means of the data processing.

7.1.2 Technology Infrastructure

Identity provider should be equipped with various technology infrastructures, such as the system designed to prevent PII leak and illegal alteration, and complete technical access control to the personal in charge of PII. The following table shows the factors that can measure the protection level for PII of the IdP from the technology infrastructure aspect.

Detailed Criteria	Description
Degree of PII protection system introduction	Checks whether the security system is introduced or not, such as the anti-virus program, firewall, IDS, IPS, and PII leak monitoring program for protecting PII.
Degree of PII protection system access control	Checks access right setting, control, and control method of each person in charge of the PII processing system.
The status of introducing encrypted PII storage and transmission	Checks encryption of major PII fields, introduction to and use status of file and DB encryption solution, and encrypted communication between user and homepage.

7.2 Protection Measures according to Identity Life Cycle

This section proposes various items that are needed to protect PII according to Identity Life Cycle. Identity Life Cycle defined in this Recommendation consists of Identity provisioning, use and maintaining, destruction.

7.2.1 Provisioning

Identity provisioning is the process to register the user and create his/her Identity with authentication information. Generally this process includes user Identity Proofing and privilege assigning to the Identity.

The standardized PII collection procedure, file that saves the PII, and management of data and output media are needed to protect the PII of the IdP at the identity provisioning phase. The following table shows the factors that can be used to measure the protection level for PII of the IdP at the identity provisioning phase.

Detailed Criteria	Description
Degree of conforming to the PII collection procedure : minimization of PII, information and consent of person	Checks whether the minimal PII is collected according to the specified, explicit and legitimate collection purpose, the PII principal whose PII are collected is informed of (1) the compulsory or optional nature of the responses, (2) the consequences of failing to give an answer, (3) the categories of persons or organizations who could eventually have knowledge of the data, and (4) the place where the right of access and rectification may be exercised and user's consent is obtained regarding PII collection and use.
Degree of PII file/data management	Checks appropriateness of the status of PII file/data management, and user notification of the PII change.

Degree of managing PII storage/output media	Checks recording of the PII use/output from the PII storage/output media, and limitation on the use of the illegal storage media.

Editor note: The assessment items needed for the identity proofing process will be added until next meeting.

7.2.2 Use and Maintaining

Identity use and maintain is the process to propagate the Identity, so that related systems can use it, and the user can use the Identity as the means of authentication and authorization when the user logs into the Relying Party. And it is the process to store and maintain the Identity and PII in the storage like the database during the retention period of it.

IdP can use the collected PII including the authentication information while using and managing the ID at the same time. Therefore, the IdP should assess access control to the PII processing system and access logging and appropriateness of information provisioning, in order to provide the PII selectively. The following table shows the factors that can be used to measure the protection level for PII of the IdP at the identity use and maintenance phase.

Detailed Criteria	Description
Access and use appropriateness of the PII processing system	Checks whether the related log information is recorded and access is controlled or not, when accessing/using the PII processing system.
Appropriateness of management when using/providing the processing information	Checks logging of the use/provisioning of the processed information, and securing security of the third enterprise and organization that is provided with the processed information.
Security of the PII	Checks whether the data controller shall take all useful precautions, with regard to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by non-authorised third parties

Editor note: The text about user consent during this process will b added until next meeting.

7.2.3 Destruction

Identity and PII destruction is the process to destroy the PII immediately after achieving the use purpose of PII or retention period, in order to prevent the unnecessary retention of PII.

The IdP may retain the PII for a certain period of time according to the IdP’s internal regulation, when the user destructs the ID or withdraws from membership. However, the IdP should destruct the PII of which retaining period is overdue, and select the proper procedure and destruction method when destroying the PII. The following table shows the factors that can be used to measure the protection level for PII of the IdP at the identity destruction phase.

Detailed Criteria	Description
Appropriateness of the PII file destruction procedure	Checks whether the PII is destructed immediately when the retaining period is overdue or the reason of destruction occurs, and the PII is destructed by the authorized person, and the user is notified of PII destruction.
Appropriateness of the PII storage media	Checks the possibility of renewing the destructed storage media, and the PII remained in the destructed storage media.
The status of retaining the PII that passed the retaining period.	Checks whether the retaining organization keeps the overdue PII in the backup date and storage media.

Editor note: Further discussion will be needed about anonymized data

7.3 Countermeasures against infringement of PII

This section presents post measures that should be taken by the IdP when the PII leak and violation incident occur, and various criteria to assess the response method, actions in question, and effectiveness of the response.

7.3.1 Measure against PII leakage on the web site of Identity Provider

If the IdP possess the web site to provide service, measures should be taken to prevent disclosure of the PII through the web site. The following table shows the factors that can be used to measure the PII level of the PII leak prevention measures taken and possessed by the IdP.

Detailed Criteria	Description
Appropriateness of PII leak prevention measures of the web site	Checks whether the PII is recorded and files are posted that could be the cause of PII disclosure through the web site, and introduction to and operation of the PII leak prevention solution.
PII exposure monitoring and vulnerabilities check	Checks whether PII leak is monitored periodically, and vulnerabilities are checked.

7.3.2 Response procedure against PII leakage

The IdP should possess the PII violation response procedure as the assessment criteria for the post measures, when the PII leak incident occurs, not to mention of preventing illegal leak of the possessed PII. The following table shows the factors that can be used to measure the protection level for PII of the post measures when the PII leak incident occurs.

Detailed Criteria	Description
The status of possessing the PII infringement incident response	Checks whether the procedure is put in place that is designed to respond to the PII leak/infringement incident occurs.

procedure	
Appropriateness of the PII infringement incident response measures	Checks whether technical/legal actions were taken after the PII leak/infringement incident occurs, and the result of taking measures is reported.
Appropriateness of the PII infringement relief procedure	Checks whether the PII infringement relief procedure is put in place, and the procedure in question is conformed.

8. PII classification criteria

The PII refers to all information that identifies or can identify the living individual. There are various types of the PII – from the information that can identify the individual such as the name, resident registration number, and passport number, to the information that can identify the individual by associating it with additional information such as the home address and phone number.

To assess the protection level for PII of the enterprise and organization, the PII possessed by the enterprise and organization in question should be classified by various criteria, and the protection level should be assessed according to these criteria. That is, the name and passport number have more possibility of personal identification than the home address and phone number, and the expected damage would be more serious when the information is disclosed. Therefore, the security measures applied to protect this information should be at a higher level than those applied to the home address and phone number. For this purpose, this standard defines the classification criteria of the PII as follows. However, detailed criteria definition and the PII type can vary, depending on the business environment of the enterprise and organization that manage the PII.

8.1 Possibility of identification

The PII can be classified whether the single information can identify the individual. For example, the name, fingerprint, and resident registration number and directly identifies the specific individual with the single information, whereas the information like the home address, phone number, and e-mail can identify the individual only when it is associated with other information, because it provides the partial information that enables to identify the individual indirectly. In addition, occupation, age, and gender cannot identify the individual, if it is not associated with the directly identifiable information. The following table shows the example of PII classification according to the possibility of identification. However, detailed criteria definition and the PII type can vary, depending on the business environment of the enterprise and organization that manage the PII.

Type	Definition and example
Directly identifiable	The information can directly identify the individual with single information, such as the name, resident registration number, passport number, biometric information, and (personally identifiable) picture, etc.
Indirectly identifiable	The information that can identify the individual only when it is associated with other PII, because single information provides the partial information to identify the individual. It includes the home address, phone number, e-mail, birthday, etc.
Unidentifiable	The information that cannot identify the individual, except when associated with

	the directly identifiable information, such as occupation, age, gender, religion, etc.

However, the unidentifiable PII can be included in the PII, as it can be used for personal identification when associated with the directly identifiable information.

Editor note: Further discussion is needed

8.2 Sensitivity of exposure

The PII can be classified by sensitivity to the damage that can occur when the signal PII is exposed, regardless of the possibility of personal identification. For example, the name and resident registration number are the directly identifiable information but less sensitive to exposure than the name and resident registration number. In addition, the credit card number is less likely to identify the individual but has high sensitivity to exposure. As described above, the PII can also be classified by sensitivity to information exposure from the perspectives of confidentiality. The following table shows the example of PII classification by exposure sensitivity.

Type		Definition and example
Single information exposure sensitivity	High	Resident registration number, passport number, credit card number, etc. (Religion is also sensitive depending on circumstances.)
	Low	Name, (personally identifiable) picture, e-mail, etc.

In addition, exposure sensitivity can increase, if signal information is combined with each other, regardless of exposure sensitivity of each PII. For example, the combination of the name and credit card number can be more sensitive to exposure than the combination of the e-mail address and credit card number. However, exposure sensitivity can vary significantly according to privacy and the service type used by the user, region, and culture, compared with other classification criteria.

8.3 Influence by the change

The influence of changing the phone number, e-mail address, and home address is not significant. However, if the PII is used as the index of the customer by the enterprise or organization, the change of the information in question is inevitably significant. The information change means illegal information forgery and alteration from the perspectives of integrity. The higher the influence of the information change, the stricter security measures should be taken.

8.4 Storage and management location

The PII also can be classified by the physical and administrative environment, such as the PII storage location and administration method. That is, the PII can be classified, depending on whether the server storing/managing the PII is located inside or outside of the organization. On the contrary, it can be determined whether the information will be managed inside or outside of the organization, depending on importance of the PII. In addition, when the PII is managed inside of the organization, it can be classified according to the scope of opening to the internal staff. For example, the sales representative may access the customer PII DB in the company to obtain the customer’s contact information. However, the important information like customer’s resident registration number should be stored and managed in such way that it can be accessed only by the sales department manager.

8.5 Access frequency

The protection of the PII can be different according to the frequency of accessing the information. For example, call center staffs access the customer’s name and phone number frequently, whereas they rarely access other PII like the customer’s e-mail address and occupation. As the exposure threat of the PII that is frequently accessed can increase in proportion to access times, higher protection level is required.

8.6 Policy/Legal ground

There can be difference in the protection level between the PII that is specified by the organization or government to be protected by the policy or law from the perspectives of confidentiality and integrity, and the one that is not specified. That is, the PII that the government specifies political /legal protection like a resident registration number requires the protection level higher than the PII that is not protected by related laws and policies like an e-mail address.

9 Criteria for assessing the level of protection for PII

The level of protection for PII can be grouped into the following 3 levels. Depending on the evaluation results of the evaluation factors specified in Section 7, the level of protection for PII can be determined as follows. However, definition of the level of protection for PII specified by this recommendation can vary according to the business policy and environment of the Identity Provider and the Relying Party

Editor Note: *This section will provide an example level of protection for PII.* **9.1 Level 1**

This is the lowest level of protection for PII. This level can be applied to service that the slight damage can occur, such as user privacy and assets, if the PII is leaked, falsified, or altered.

9.1.1 Infrastructure

[TBD]

9.1.2 Protection Measures based on Identity Life Cycle

[TBD]

9.1.3 Countermeasures against infringement of PII

[TBD]

9.2 Level 2

This is the middle level of protection for PII. This level can be applied to service that the serious damage can occur, such as user privacy and assets, if the PII is leaked, falsified, or altered.

9.2.1 Infrastructure

[TBD]

9.2.2 Protection Measures based on Identity Life Cycle

[TBD]

9.2.3 Countermeasures against infringement of PII

[TBD]

9.3 Level 3

This is the highest level of protection for PII. This level can be applied to service that the fatal damage can occur, such as user privacy and assets, if the PII is leaked, falsified, or altered. Therefore, the level 3 systems and services require complete system availability and PII management.

9.3.1 Infrastructure

[TBD]

9.3.2 Protection Measures based on Identity Life Cycle

[TBD]

9.3.3 Countermeasures against infringement of PII

[TBD]

10 Conformance Guidelines for determining the level of Protection for PII

Editor Note: *Suggest the guideline designed to determine the level of protection for PII in the Identity Provider, compared with the level defined previous section.*