A Practical Trust Framework: Assurance Levels Repackaged Through Analysis of Business Scenarios and Related Risks

Masatoshi Hokino[1], Yuri Fujiki[1], Sakura Onda[1], Takeaki Kaneko[1],
Natsuhiko Sakimura[2], and Hiroyuki Sato[3](✉)

[1] JIPDEC, Tokyo, Japan
{hokino-masatoshi,fujiki-yuri,onda-sakura,kaneko-takeaki}@jipdec.or.jp
[2] Nomura Research Institute, Tokyo, Japan
n-sakimura@nri.co.jp
[3] The University of Tokyo, Tokyo, Japan
schuko@satolab.itc.u-tokyo.ac.jp

Abstract. In cyberspace, standards for the expression of the trustworthiness of identities have been developed by various parties. This trustworthiness is often referred to as entity authentication assurance, and its degree is often called LoA (levels of assurance, or assurance levels). There are two prominent LoA standards: NIST SP800-63-2 and ISO/IEC 29115:2013. LoAs are designed to express different levels of assurance. Multiple viewpoints are set in assessment, and related assessment criteria for each viewpoint are packaged into one LoA. For deployment of LoAs in enterprise business scenarios, the choice of assessment criteria in a given LoA must match the specific business requirements. We perform a field survey on business scenarios in which trust in identities is a major problem. In the survey, we focus on two key factors of assessment: identity proofing and authentication process. In addition, we observe the overall fit and gap in business scenarios. Results indicate that raising the assurance of the authentication process is effective for raising the overall assurance level. Based on the investigations performed, we repackage light weight identity proofing and LoA 2 equivalent credential management and usage into a new assurance level, LoA 1+, for the "right" cost benefit balance.

1 Introduction

The importance of trusted identities in cyberspace has become widely recognized in recent years. Standards for the expression of the trustworthiness of identities have been developed by various parties. Many government led activities exist, e.g., FICAM TFPAP [6] and NSTIC [14] of the U.S.A., GOV.UK Verify of U.K. [7], etc. While some of these activities are for government use, others do target both efficient e-governments and more efficient commercial sector activities promoting the formation of new industries.

In the case of FICAM TFPAP [6], major objectives include the establishment of well-defined identity and credential management at the identity provider (IdP)

L. Chen and S. Matsuo (Eds.): SSR 2015, LNCS 9497, pp. 203–217, 2015.
DOI: 10.1007/978-3-319-27152-1_11

which is proportionate to the risk of compromise of the business that consumes the resulting identities, referred to as the relying party (RP). The identity that is conveyed from an IdP to an RP is called “federated identity” and a group of such IdPs and RPs are called a “federation.” To establish mutual trust among the participants, technical and operational standard should be followed. The trust establishment also requires enforcement functions for violators. The combination of these “tools and rules” is referred to as a “trust framework.”

A trust framework enables its stakeholders to trust claims made from the other stakeholders under condition of information asymmetries. For example, when an IdP provides a set of attributes related to an entity to an RP, in general, it has no means of evaluating the trustworthiness of the information that it receives. Under such circumstances, the transaction will typically not occur and the market breaks down, as shown in the Market of Lemons introduced by [1].

Establishing a measurement unit for the quality of identities along with a kind of operational framework that assures the truthfulness of the providers would be a solution. The trust framework can be applied for this purpose.

In order for a trust framework to be practical, it must be applicable to a variety of business scenarios. To express the required assurance level that is proportionate to the risk of the RP’s business, the concept of LoAs (level of assurance, or assurance level) have been introduced. An RP requires a level of assurance as the minimum requirement under which it can accept identities from an IdP. Furthermore, an IdP will provide such identities if it can. Standardizing this expression in a small number of variance enables the trust framework to scale up the participation, which is an important requirement for cyberspace applications.

There are many standards that define the aspects of LoAs. The combination of OMB M-04-04 [16] and NIST SP800-63-2 [3] is a prime example. It defines four levels of risks and corresponding LoAs. However, the adoption of these standards in the private sector is not widespread, possibly because the requirements are focused towards the U.S. government entities and its direct adoption is difficult for private sector entities especially those outside U.S.

ISO/IEC 29115 [9] generalizes the older version of NIST SP800-63-2 that originally targets the US government usage. It reflects the demand of extending trust frameworks to business scenarios. Unlike NIST SP800-63-2, it does not mandate the use of government issued photo IDs nor trusts such IDs. It is more risk based and process oriented. Only photo IDs produced in a documented process deemed to produce a sufficient confidence in the document are trusted. While this certainly expands the scope of applicability, the adoption is still not widespread in the private sector. One of the reasons appears to be that for most business, LoA 2 and above are not cost effective.

In this paper, we begin our examination from the fact that both standards set multiple viewpoints in assessment, and package assessment criteria for each viewpoint into one LoA. The choice of assessment criteria in a given LoA must be examined to discover the match of business requirements.

First, we examine business use cases to determine possible reasons for low adoption of the standards. Next, we undertake a field survey on business scenarios in which trust in identities represents a major problem. The survey focuses on two key factors of assessment, identity proofing and authentication process, and observe the fit and gap for those business scenarios.

From the investigation, we repackage light weight identity proofing and LoA 2 equivalent credential management and usage into a new assurance level, LoA 1+ for the "right" cost and benefit balance.

As the result, we show that the process of field survey, investigation and repackaging is a subject of engineering.

The rest of this paper is organized as follows: Sect. 2 surveys related work and standardization. In Sect. 3, we analyze the assessment criteria of existing standards. In Sect. 4, we explain our field survey of business scenarios. In Sect. 5, we discuss LoA 1+, and the repackaging process based on the result of Sect. 4. Section 6 concludes this paper.

2 Related Work on Trust Framework

The majority of identity trust frameworks have two facets: technical requirements that define LoAs and operational rules that ensures the adherence to the technical requirements. This combination is often referred to as "tools and rules."

Technical requirements are further decomposed into a credential issuance process that includes identity proofing and an authentication process. Identity proofing and related issues (especially privacy) is discussed in [19]. In [13], the assurance of authentication is described.

Until now, there have been a number of technical proposals related to trust frameworks and assurance levels. In [29], assurance of attributes has been proposed in addition to assurance of authentication. [30] gives a discussion of digital identities in general. Today, assurance levels are considered a topic of engineering which includes trust elevation [15,18] that aims at collecting evidence of low assurance in order to give higher assurance. Furthermore, [17] proposes a fine tuning of assurance levels. However, such proposals need to be applied to enterprise business scenarios to obtain feedback for standardization. In this regard, standards for operations of practical trust frameworks are of high significance.

The U.S. has a long history of defining LoAs. The combination of OMB M04-04 [16] and NIST SP800-63-2 [3] sets risk and control criteria for building a trust of governmental agencies. From their inception, multiple levels are incorporated to cover a wide spectrum of trust ranging from id/password authentication to PKI.

Japan has also created the guidelines for risk analysis, digital signing and authentication for on-line applications and processing [4].

ISO/IEC 29115 [9] and its ITU-T version ITU-T X.1254 [10] are a framework for managing assurance levels of entity authentication. As in NIST SP800-63-2, four assurance levels and criteria are defined. In all of these, a final level of assurance is defined as the lowest of the process.

[2] discusses identity assurance in another scheme that includes the audit process.

Deployment of this kind scheme for the healthcare sector is discussed in [5].

3 Assessment Criteria of Assurance Levels

There are two significant standards for the assessment of assurance levels: NIST SP800-63-2 and ISO/IEC 29115.

This paper focuses on identity proofing, credential issuance, and the authentication process in the set of assessment criteria.

3.1 Credential Issuance and Identity Proofing Process Requirements

In both standards [3,9], the identity proofing process is defined as a prerequisites for the issuance of credentials. Here, concrete threats are analyzed, and controls corresponding to each threat are considered.

At the credential management phase, there is some difference in the levels of protection as shown in Table 1.

Table 1. Controls on credential management

Level	Control at issuance	Secure storage
1	–	access control
2	mechanism to protect the credential from being handed to a wrong person	not to be stored in clear text
3	stricter mechanism to protect the credential from being handed to a wrong person	mechanism to protect the credential

As most modern systems provide a secure mechanism to protect credentials, there is little difference in the evaluation at this point. In practice, the most difference is derived from the identity proofing process. NIST SP800-63-2 and ISO/IEC 29115 define similar criteria. Table 2 shows ISO/IEC 29115 identity proofing objectives and controls.

Nonetheless, there is only a slight difference between NIST SP800-63-2 and ISO/IEC 29115. As NIST SP800-63-2 is created to meet the requirements of the U.S. government, where with most government related uses, there is a requirement to map the identity at the front door of the service to the identity stored in the backend database, using such identifying attributes such as name, date of birth, gender, and address as the keys. Because mis-matching of the keys would cause risks, in higher levels, showing “government issued” identity documents is demanded, They are more likely than others to include those “keys” that correctly map to the governmental backend database. Furthermore, the U.S.

Table 2. Requirements of identity proofing in ISO/IEC 29115 (Summary)

Level	Objectives	Controls
1	Self-claimed or self-asserted	Self-claimed or self-asserted
2	Identity is unique within context and the entity to which the identity pertains exists objectively	Proof of identity through use of identity information from an authoritative source
3	Identity is unique within context, entity to which the identity pertains exists objectively, identity is verified, and identity is used in other contexts	Proof of identity through use of identity information from an authoritative source + identity information verification

government typically knows the quality of the government issued identity documents. In Table 2, the "authoritative source" is replaced with "government" in NIST SP800-63-2.

On the other hand, ISO/IEC 29115 aims at being useful to the private sector internationally. In private sector use cases, it does not often matter whether the business exactly knows the customer's real name and date of birth or other attributes. Instead, it is more important to know whether that person has actually completed payment, which is the decisive factor for the entitlement of that specific service. As a result, ISO/IEC 29115 introduces the concept of "policy compliant identity document." The attributes to be proofed and verified depend on the business context. The business should document them according to the policy.

Another aspect of ISO/IEC 29115 is its tendency to be more process oriented. In an international context, there are government issued identity documents that are sometimes produced by low-quality processes. Such identity documents are not trustworthy even if they have been issued by an agency of government. This is another reason why ISO/IEC 29115 is asking for "policy compliant" identity documents that have adequately addressed the threats.

3.2 Authentication Process Requirements

In the standards [3,9], there are specified requirements for the authentication process. There are a number of proposed and deployed authentication mechanisms and processes which include passwords, one-time passwords, biometrics, and public key authentication. Their risks have been analyzed, and as a result, the strength of each authentication method can be objectively discussed.

NIST SP800-63-2 not only sets the threat that each LoAs should mitigate, but it maps specific type of credentials to be used for each LoAs.

ISO/IEC 29115 takes a slightly different approach. Instead of assigning specific types of credentials to each level, it only presents the technical requirements. ISO/IEC 29115 does not specify the credential type to accommodate the combination of various techniques. Furthermore, there is a specified control selection in the credential usage. Reflecting that any number of combinations of those controls can be used to mitigate the specific risk, it does not specify what has to be done at each level, but leaves those decisions for implementation.

3.3 Requirements for Certification

To establish a trust framework, only defining the levels of assurance is not sufficient. A trust framework must define a mechanism that provides a sufficient level of confidence of the members' adherence to the rules.

The combination of FICAM TFPAP [6] and certified trust frameworks such as Kantara Initiative Identity Assurance Program [12] are prime examples of such works. This combination lays out the audit requirements for each level of assurance. A third party audit is required for any levels including and above LoA 2.

Similarly, InCommon Federation [8] provides a program for certifying levels, while federations in Europe and Japan provide a limited program of certification.

4 Analysis of Business Scenarios in Terms of Assurance Levels

As NIST SP800-63-2 is designed for use by federal agencies, its applicability to the private sectors is limited in nature. The design of ISO/IEC 29115 is more generalized. However, its usefulness to the private sector has yet to be thoroughly investigated. Especially because they have a structure of packaging requirements of different viewpoints, this structure should be examined to determine whether the combination of requirements in the standards is appropriate, or covers a wide range of businesses. To identify the fit and gap, we have conducted a field survey in Japan to identity applicable business scenarios for trust frameworks.

4.1 Design Objectives of Field Survey

The objectives of this field survey is to identify the structure of assurance levels in terms of cost and effectiveness. In previous sections, we have presented that the structure of assurance levels is determined by the identity proofing and authentication processes together with the objectivity of the assessment.

Therefore, in order to have an appropriate coverage of business sectors. the survey has collected a wide range of business scenarios that are consumer oriented and where identity proofing is either legally required or required through industry self-regulation.

The data collected for each business type is listed below:

Market size this reflects the influence that the business sector has on the economy. This data is basically from [26].

Business practice (on-line/off-line/both) off-line business practice is also included because it is a future on-line business candidate, and the importance is not affected by the business practices.

In terms of assurance levels, we have collected the information below:

Authentication method/process criteria defined in [6] are used. In the criteria, the method of identity proofing is classified as non-technical, and shows the most conspicuous difference between levels. The criteria of identity proofing for levels 1 to 3 listed in Table 2 are used.

Regulations some processes are enforced by law. For example, in Japan, when opening a bank account, the identity proofing of level 2 is required by law. However, even if there are no regulations, some industry associations define self-regulation of identity proofing to achieve safer transactions and to protect the reputation of the business. in this survey, both processes enforced by law and processes self-regulated by industry associations have been collected.

As regulations are closely related to the quality (objectivity) control of the assessment, we also discuss this problem in Sect. 4.3.

4.2 Classification of Business Scenarios

Combining both evaluation criteria in terms of business type and assurance levels, the classification of services surveyed is presented in Table 3.

In Table 3, the first column expresses the levels of identity proofing. Services classified as 1-{1, 2, 3, 4} require level 1 identity proofing. Similarly, services classified as 2, and 3 require level 2, and level 3, respectively.

For services that require level 1 identity proofing, we have found that there are different regulation stipulations which are given a separate class listing from 1-1 through 1-4.

In examining the table, some significant categories begin to emerge:

1. The first category is the case where identity proofing is entirely self asserted. In this category, customers are requested to fill their information by themselves. There is no stipulation on identity proofing. This category is marked as 1-1. In the case of a hotel stay, the customer is required by the Inns and Hotels Act to inform the hotel one's true identity. Failure to do so may result in detention of less than 30 days or a fine of less than JPY 10,000.
   Note that this category contains scenarios whose business size is very large.
2. In the second category, some kind of identity proofing is required either by law or self-regulation, it is not strictly enforced in practice. Here, a wide range of identity proofing processes are adopted. Examples include checking photo ID in any form. This may include the IDs that are not issued by the government (e.g. student ID issued by a university), and inspecting the validity of a credit card. For business processes that only require age verification, an identity document is requested only in cases where the age is under suspicion. In these cases, the identity proofing method is often specified by the self-regulatory bodies, not by law. Penalties for being non compliant seems to be relatively minor. (marked from 1-2 through 1-4).

Example 1 (horse racing†). In Japan, by law, minors under the age of 20 are not allowed to bid on horse races. However, the method of identity proofing is not stipulated. The promoters perform the identity proofing by inspecting the

Table 3. Classification of businesses by types of identity proofing regulation

Class	Services	on-line/off-line	Size (M JPY)	Regulation (Publication of self-regulation on identity proofing by industrial association ✓)	
1-1	Hotel booking	both	4,045,618	Customers are required to fill out the name and address form (self-assert)	
	On-line shopping	on-line	[24] 12,800,000	practice not stipulation	✓
	On-line games	on-line	[23] 577,100		✓
1-2	Gov.controlled gambling†	on-line	1,834,110		✓
	Sport based lottery	on-line	^{a}110,797		✓
	Shopping (tobacco, liquor)	on-line	1,741,853	minors are not allowed	
	Late show (cinema, karaoke)	offline	^{b}319,329	(practice not stipulated)	
	adult (cinemas, magazines)	on-line	N/A		
1-3	Rental (video, autos, etc.)‡	both	1,867,196		
	Certification	offline	N/A	identity proofing required	
	Shopping (tobacco)	offline	150,539	(practice by self-regulation)	
	Marriage matching	on-line	18,167		✓
1-4	On-line dating	on-line	N/A	identity and age proofing required	
	Pawnshop	offline	N/A	(practice stipulated)	
2	Cell phones§	both	^{c}6,775,517		
	Bank account		[11] 15,881,400		
	Life insurance		[21] 41,981,800		
	Non-life insurance		[20] 9,667,900	identity proofing required	
	Credit card	offline	[22] 57,069,076	(enforced by law)	
	Real estate brokerage		9,824,601	(practice stipulated)	
	Precious metal trading		444,552		
	Secondhand articles dealer	on-line	303,844		
	Private office		N/A		
	Hotel booking (for foreigners)		^{d}4,045,618		
3	Digital certificate issuance	on-line	227,993		

Unless specified, from [26].
$^{(a)}$ Official publication of the Sports Promotion Lottery "Toto."
$^{(b)}$ total market size (not restricted to late show)
$^{(c)}$ Calculated by reference to [25]
$^{(d)}$ total market size (not restricted to foreigners)

credit card presented. A significant penalty exists for mis-identification. Promoters knowingly selling the race tickets to a minor will be subject to a fine of less than JPY 500,000 (Horse Racing Law[1], Article 34).

Example 2 (DVD rental‡). In Japan, there is no legal requirement for identity proofing in the DVD rental business. However, some business sectors voluntarily define regulations in which identity proofing should usually be performed by using photo IDs issued by public sectors.

[1] Horse Racing Law (in Japanese) http://law.e-gov.go.jp/htmldata/S23/S23HO158.html.

Table 4. Mapping identity proofing requirements of types of businesses to FICAM and ISO LoAs

Class	Evidences/procedures used by the business	FICAM LoA	ISO LoA
1-1	Self-Claimed	1	1
1-2	Documented procedure on Authoritative Sources[a]		2
1-3	Inspection of Photo ID (non-government ID allowed)		
1-4	Inspection of publicly issued documents		
2	Government Issued[b]Photo ID inspection	2	
3	Government Issued[a]Photo ID validation	3	3

[a] In case of age confirmation, IDs may not be required where determination is obvious,

[b] Depending on the business, some government issued photo IDs are not accepted.

3. Additional categories require the identity proofing methods corresponding to levels 2 and level 3 (marked as 2 and 3, respectively in Table 3). Most of these identity proofing processes are required by Japanese law.

Example 3 (cell phones§). To purchase mobile phones in Japan, a customer is required to show a government issued photo ID for identity proofing, or at least two pieces of evidence from public services for the proofing of one's name and address. Furthermore, the customer's address is verified by sending something to that address using the postal service. This is a typical process of identity proofing for assurance level 2.

By analyzing identity proofing processes of typical business scenarios, we can conclude that the criteria defined for government use [6] or the ISO standard [9] could also be used in many business scenarios.

Table 4 maps the identity proofing level of each category to the FICAM TFPAP and ISO/IEC 29115 LoA.

Note that the classification in Table 4 is based on the assurance levels of FICAM, which is represented by the matching of the major number of class and the FICAM LoAs.

However, these findings highlight differences to ISO LoAs in level 1 and 2. Actually, ISO/IEC 29115 expands the types of evidence of identity to accommodate private sector reality. On the other hand, however, it does not necessarily accept government issued identity documents. The difference lies in the importance of the process adopted during the creation of the document. This explains the fact that some businesses in Japan do not accept certain kinds of identity documents issued by some government agencies because they consider the possibilities of fraudulent issuance of those identity documents unacceptably high. This would not happen for government agencies, because any document produced by another governmental body is deemed accurate under Japanese law.

What is important, however, is that the identity proofing methods adopted by each class are covered by the ones specified by FICAM or ISO/IEC, even if we find some differences between the two.

In the remainder of this paper, we present our proposal to adopt the identity proofing methods of ISO/IEC 29115 to design a new class of assurance levels.

4.3 Self-Regulation and Objectivity

Table 3 includes the survey of the self-regulations. The objectivity of a claim is a common issue of self-regulations. Using independent audit or assessment is counted as a solution, which has still a problem on cost.

In Table 3, we see that some of them make effort in defining and publishing their own regulation as a form of their industrial associations (marked with ✓), which raises assurance of adherence to the regulation.

4.4 Effectiveness of High Level Authentication Processes

From the survey results of Sect. 4.1, use cases fall under ISO/IEC 29115 LoA2 and above are clustered as an important economic sector. However, we should not dismiss the cluster of businesses in Class 1-1 which correspond to ISO/IEC 29115 LoA 1. The mere fact that the market size of on-line shopping entities of Class 1-1 far exceeds that of shopping at the LoA 2 and 3 indicates its importance.

On-line games are an example of one such service and their prevalence merits analysis. The second survey is a case study on the effectiveness of raising assurance of an authentication processes.

On-line games are usually considered privacy sensitive. Our survey has found that the identity used there are usually self asserted. However, attacks that use previously collected username and password pairs from elsewhere, referred to as a list-based attack, saw a sharp increase in 2011. Statistics showed that some content providers in Japan received over 200,000 attacks per month.

A press release from the National Police Agency (NPA) on March 4, 2010 states:

Notes on the prevention of illegitimate access. Access controllers should improve their security (e.g. improving user authentication through introduction of One-Time-Password)

Actions to be taken by the NPA. NPA should influence the businesses (e.g., On-line game providers and Internet banks) by requesting them to improve the user authentication method.

Responding to the request by the NPA, the Japan On-line Games Association (JOGA) started operating a shared identity platform and helped each on-line game provider to adopt a two factor authentication process. This platform helped greatly to reduce the introduction and operation costs for each provider. In addition, if the provider uses the platform, any economic damage incurred from account compromise will be covered. Today, this platform is widely used by many game providers in Japan.

From a game user's standpoint, using the same authenticator across providers has reduced the difficulty of provider-wise authentication. Moreover, the fact that there is a reimbursement for account compromise seems to have made the acceptance rate high, which offsets any additional actions required by the platform.

The "On-line Game Security Guideline" published by JOGA on August 15, 2012 [28] contains the following points:

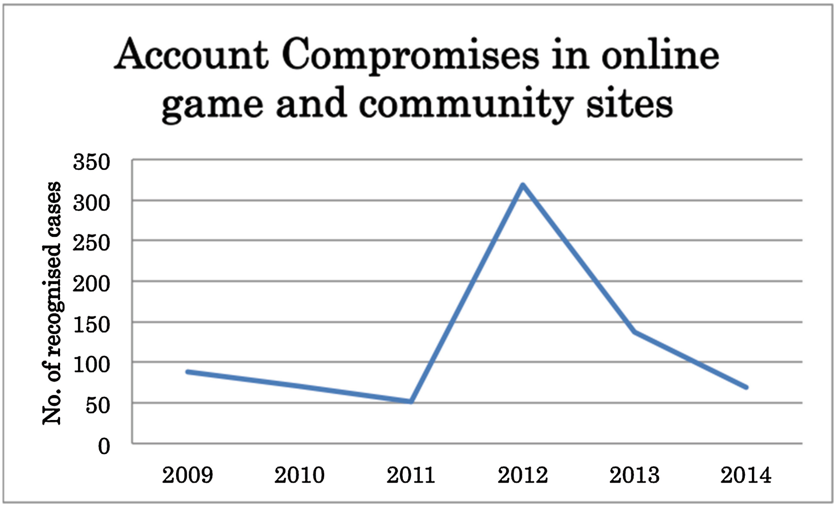

Fig. 1. Account compromises in on-line game and community sites

- Information Sharing guidelines when a security incident occurs,
- Guidelines for dealing with list-based account cracking,
- Security Solution Guidelines for One-Time Password etc., and
- Guidelines on coordination with security vendors and related associations.

As shown in Fig. 1, the introduction of the guidelines, in conjunction with the higher assurance authentication measures drastically led to a decrease in the number of incidents and countered the increasing trend of account compromise, this showing marked improvement. The data of Fig. 1 is taken from the series of annual reports published by the National Police Agency from 2010 to 2015 [27]. The reports published in March each year cover incidents for the previous year. In 2013, a 56 % decrease compared to 2012 is observed, and in 2014, a 78 % decrease is observed.

On-line games are classified as Class 1-1. This indicates the significance and usefulness of combining higher level authentication measures with a lower identity proofing level. This practice is distinguished from the business scenarios that use lower security authentication measures with the same level of identity proofing. Thus, even when low level identity proofing is adopted, high assurance authentication measures can be used effectively to raise security. In addition these results prove that there are some authentication measures which support high assurance levels and are also cost-effective.

However, in neither SP800-63 [3] nor ISO/IEC 29115 [9], the difference between "self-claimed identity proofing + low security authenticator" and "self-claimed identity proofing + higher security authenticator," cannot be distinguished despite the latter being useful for risk management.

Thus, we have identified a new class of assurance levels: low assurance in identity proofing and high assurance in authentication process. We conclude that the results from these surveys call for a new category of level of assurance: LoA 1+.

Table 5. LoA table

LoA	Level of identity proofing (as of ISO/IEC 29115)	Level of authentication (as of ISO/IEC 29115)
1	level 1	level 1
1+	level 1	level 2
2	level 2	level 2
3	level 3	level 3

5 Level of Assurance 1+

As discussed in the previous section, the results of our survey suggest the creation of a new assurance level is useful for important business sectors. However, as a natural request, the criteria for assessment must be simply organized, and that a rise in security level should be easily understood. Therefore, we propose the creation of a new assurance level by re-packaging components of assessment criteria. To further justify this, we consider identity proofing, authentication method/process, and objectivity assurance.

In the previous section, we have shown that in level 1 (self-assertion) in identity proofing, a higher security authentication method can be a factor for raising security. Here, our proposal departs form the idea of taking the "minimum level" of the processes as the resulting LoA, and we define LoA 1+ as the one requiring higher authentication process, while keeping the level of identity proofing the same as LoA 1. The result of this re-packaging is shown in Table 5.

Note that there is no combination of level 2 and above for identity proofing with a low level authentication process (specifically, level 1). There is no point of using those combinations because if the level of authentication is low, the resulting identity may be compromised even if higher level identity proofing is adopted.

The following examples examine the kind of business scenarios that can be entitled to LoA 1+ in order to achieve their advanced security.

Statistics from JOGA [28] justify the effectiveness of adopting LoA 1+. Thus, we can conclude that LoA 1+ meets the requirements of JOGA, and verifies its effectiveness in preventing fraudulent use in on-line shopping and on-line game sites. Moreover, these businesses can claim higher security by acquiring a new LoA certification which is stronger than LoA 1.

Table 3 shows that on-line shopping and games are classified as 1-1 (lowest), yet have a significantly large market size. By acquiring LoA 1+, these businesses can claim that their security is higher than 1-1.

Certification Requirement. For operating LoAs in a given trust framework, it is important that some assurance is given related to the policy compliance. As seen in Sect. 4.3, service providers pay attention to acquiring trust in their business. Obtaining public certification and announcements of their policies and procedures are usually used for this purpose.

In trust frameworks obeying FICAM TFPAP, such assurance is given by attestation through an independent audit performed by designated assessors. The separation is drawn between LoA 1 and LoA 2, in that, an independent audit is required by FICAM TFPAP to obtain LoA 2 certification. While an independent audit gives objectivity to one's claim, however, it also incurs a higher operation cost.

However with LoA 1, because the identity proofing is based on self-assertion, there is not much to audit and an objective external/independent audit is not required. However, there is inherent limitation in objectivity.

In the case of LoA 1+, the identity proofing situation is the same as in LoA 1, but relying parties may want to have some assurance as to the trustworthiness of the authentication measure used there.

The control that we propose in this paper is to adopt a reputation model to build trust. More specifically, we propose to have the operating body publicly announce the operating policies, procedures and its adherence to them. The procedures themselves will be the target of public evaluation. If an operating body does not operate as declared, it will face a reputation risk as well as other legal consequences. Furthermore, there is made some effort such as endorsement by related industrial associations that can be considered as a kind of cost effective social system for assurance raising.

As discussed in the last section of the survey, this reputation model is widely adopted and has proved effective to some extent. We conclude that this model is enough for an operating body to keep itself compliant with the policies and procedures declared in advance. Table 6 summarizes this discussion.

Table 6. Certification requirement for each LoA

LoA	Requirement	Grounds
1	No requirement	–
1+	No requirement	reputation risk
≥2	External/independent audit	objectivity

6 Concluding Remarks

In this paper, we have first analyzed the assessment criteria of existing standards of FICAM and ISO/IEC 29115, examining the key factors of identity proofing and authentication process. Next, conducting a fit and gap survey of various factors in business scenarios, we have listed typical instances with their characteristics and market size together with the adopted identity proofing and authentication process. In the analysis, we have discussed and proposed the creation of a new class of assurance level, which we refer to as LoA 1+ formed by re-packaging components of existing standards to serve an important business type.

Results from our survey have shown that conventional LoAs are useful in many situations. However, our data indicates that conventional LoAs have overlooked an important category of use case: the combination of self-claimed identity and high level authenticator. While the market sizes of the sectors that rely on self-claimed identity are huge, they face significant risk as shown in the on-line games case. Data from that example has proved that it is possible to significantly reduce the risk by just upgrading the authentication process without upgrading the identity proofing process. Observing these results, we have proposed a repackaging of existing LoA framework and created LoA 1+ that combines self-claimed identity and high level authentication.

It is also important to address the information asymmetry. While an identity provider may claim that it has used a high level authenticator to authenticate the user, it may well not be the case. A third party audit would be certainly effective to prove the claim, but this is a heavy weight process. Instead, we have proposed to rely on transparency and reputation risk for compliance of LoA 1+.

This level of assurance seems to fulfill trust and security requirements both from the service providers and from the users as evident in the on-line games use cases. Other industries are likely to benefit from following a similar strategy in adopting the LoA 1+ entity authentication assurance level.

References

1. Akerlof, G.A.: The market for “lemons”: quality uncertainty and the market mechanism. Q. J. Econ. **84**(3), 488–500 (1970)
2. Baldwin, A., Mont, M.C., Beres, Y., Shiu, S.: On Identity assurance in the presence of federated identity management systems. In: Proceedings of the International ACM Workshop on Digital Identity Management 2007, pp. 27–35 (2007)
3. Burr, W.E., Dodson, D.F., Newton, E.M., Perlner, R.A., Polk, W.T., Gupta, S., Nabbus, E.A.: Electronic Authentication Guidance. NIST SP 800–63-2 (2013)
4. Cabinet of Japan: Guideline for Risk Analysis, Digital Signing, and Authentication for On-line Applications and Processing (2010) (in Japanese). http://www.kantei.go.jp/jp/singi/it2/guide/guide_line/guideline100831.pdf
5. Coats, B., Acharya, S.: The forecast for electronic health record access: partly cloudy. In: Proceedings of the IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, pp. 937–942 (2013)
6. Federal Identity, Credential, and Access Management Trust Framework Solutions: Trust Framework Provider Adoption Process (TFPAP) For All Levels of Assurance (2014). http://www.idmanagement.gov/sites/default/files/documents/FICAM_TFS_TFPAP_0.pdf
7. GOV.UK: Introducing GOV.UK Verify (2015). https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify
8. InCommon: The inCommon Assurance Program. http://www.incommon.org/assurance/
9. ISO: ISO/IEC 29115:2013, Entity authentication assurance framework (2013)
10. ITU-T: Recommendation X.1254, Entity authentication assurance framework (2012)
11. Japanese Bankers Association: FY2013 Financial Statements of All Banks (2014)

12. Kantara: Identity Assurance. https://kantarainitiative.org/idassurance/
13. Noor, A.: Identity protection factor (IPF). In: Proceedings of the IDtrust 2008, pp. 8–18 (2008)
14. NSTIC: National Strategy for Trusted Identities in Cyberspace. http://www.nist.gov/nstic/
15. OASIS: Electronic Identity Credential Trust Elevation Framework V 1.0 (2014). http://docs.oasis-open.org/trust-el/trust-el-framework/v1.0/trust-el-framework-v1.0.pdf
16. Office of Management and Budget: M-04-04: E-Authentication Guidance for Federal Agencies (2003)
17. Sato, H.: $N \pm \epsilon$: reflecting local risk assessment in LoA. In: Meersman, R., Dillon, T., Herrero, P. (eds.) OTM 2009, Part II. LNCS, vol. 5871, pp. 833–847. Springer, Heidelberg (2009)
18. Sato, H.: A formal model of LoA elevation in online trust. ASE Sci. J. **1**(4), 166–178 (2012)
19. Slomovic, A.: Privacy issues in identity verification. IEEE Secur. Priv. **12**, 71–73 (2014)
20. The General Insurance Association of Japan: Income Statement (2015) (in Japanese)
21. The Life Insurance Association of Japan: Life Insurance Fact Book 2014 (2014) (in Japanese)
22. The Ministry of Economy, Trade and Industry: 2013 Survey of Selected Service Industries (2014) (in Japanese)
23. The Ministry of Economy, Trade and Industry: Digital Content White Paper 2014 (2014) (in Japanese)
24. The Ministry of Economy, Trade and Industry: Market Research on Electronic Commerce 2015 (2015) (in Japanese). http://www.meti.go.jp/press/2015/05/20150529001/20150529001-3.pdf
25. The Ministry of Internal Affairs and Communications: White Paper on Information and Communications in Japan (2014) (in Japanese)
26. The Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry: 2012 Economic Census for Business Activity (2012) (in Japanese)
27. The National Police Agency (2010–2015) (in Japanese). https://www.npa.go.jp/cyber/statics/h2{2-6},/pdf041.pdf
28. Third Networks Co.: JOGA Security System for On-line Games and Smartphone Games (2011) (in Japanese). http://www.jssec.org/dl/111117_4_amemiya.pdf
29. Thomas, I., Meinel, C.: An attribute assurance framework to define and match trust in identity attributes. In: Proceedings of the 2011 IEEE International Conference on Web Services, pp. 580–587 (2011)
30. Yong, J., Bertino, E.: Digital identity enrolment and assurance support for VeryIDX. In: Proceedings of the 14th International Conference on Computer Supported Cooperative Work in Design, pp. 734–739 (2010)