



ISO/IEC JTC 1/SC 27 **N6059rev1**

ISO/IEC JTC 1/SC 27/WG 5 **N56059rev1**

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: national body contribution

TITLE: USA NB contribution received on document SC 27 N5875 -- ISO/IEC 1st WD 29115 -- Information technology -- Security techniques -- Authentication assurance

SOURCE: ANSI, National Body of United States

DATE: 2007-09-12

PROJECT: 29115

STATUS: This document has been revised and is being re-circulated as SC 27 N6059rev1 for consideration at the 3rd SC 27/WG 5 meeting in Lucerne (Switzerland) on 1st - 5th October 2007.

ACTION ID: ACT

DUE DATE:

DISTRIBUTION: P, O, L Members
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice-Chair
E. J. Humphreys, K. Naemura, M. Ohlin, M.-C. Kang, K. Rannenber, WG-Conveners
D. Brackney, Project Editor

MEDIUM: Livelink-server

NO. OF PAGES: 1 + 21

Date: 2007-08-13	Document: SC27 N5875
------------------	-----------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
US 1	Title		Te	The title of this proposed standard does not reflect the scope of the standard. The current scope includes identity proofing, identifier types, and privacy. These are topics normally associated with Identity Assurance (IdA) vs. Authentication Assurance. Consequently, the current scope is much broader than authentication assurance that is a subset Identity Assurance (IdA).	In the title, Change “Authentication” to “Identity”	
US 2	General		Te	Both ISO/SC27 and ITU-T are in the process of developing IdM related standards and IdA is a critical component of IdM. A common text ITU-T Recommendation ISO/IEC International Standard and for Identity Assurance (IdA) would be a more efficient use of the limited resources that are available in ISO/SC27 and ITU-T SG 17 to develop the standard. The proposed common text IdA standard will improve and enhance the trust and confidence in the identity life cycle to include authentication assurance. It will also help minimize the current fragmented way in which digital identities are addressed today. Because SC27 is in the early stages of	Change this ISO Standard to a Common text ITU-T Recommendations ISO/IEC International Standard in accordance with the procedure and format given in ITU-T’s Rec A23, JTC 1 Directive, Annex K and the Word Template. Rules for presentation of ITU-T Recommendation ISO/IEC International Standard are provided in Guide for ITU-T and ISO/IEC JTC1 Cooperation These documents provide the basis for collaborating in the development of a Common Text	

1 MB = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 Type of comment: ge = general te = technical ed = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
				developing this standard, the project milestones should not be effected..	Standard.	
US 3	Scope	1 st para last sentence	Te	Clarify scope	Change "... applicable to a wide range of authentication mechanisms." To "...the entire life cycle of an identity."	
US 4	Scope	2 nd para	Te	Clarify scope	Replace sentence before the bullet list in the 2 nd para with the following: This objective of this standard is to describe a set of guidelines that should be considered in assessing "how" close" an identity is to the correct one throughout an identity's life cycle. This assessment takes into account the following: <i>Use existing bullet list</i>	
US 5	Definition	New Para	Te	Clarify scope	Add the following paragraph at the beginning of the Introduction Clause. Identity Assurance (IdA) involves technologies and processes to ensure that identity management (IdM) security controls are	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Date: 2007-08-13	Document: SC27 N5875
------------------	-----------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
					<p>sufficient to make sure that an entity has confidence that the entity at the other end of an authentication transaction is who or what they say they are. IdA is the ability to associate identity attributes (email address, IP address, etc.) to an entity and the secure management and protection of this data. IdA is concerned with the proper risk associated with IdM to include the authentication process.</p> <p>IdA consists of determining that an individual seeking a credential is who they say they are. Among other things, IdA involves the identity registration process. In order to determine that an individual seeking a credential is who they purport to be, it is necessary to first establish a history of identity by collecting identity information (e.g. biometric and biographical information). The next step is to validate the accuracy and legitimacy of the information collected and</p>	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
					<p>verifying the identity source documents. The final step in identity proofing is ensuring that identification credentials are provided only to correct individuals.</p> <p>The goal of authentication assurance or Quality of Authentication (QoA) is to quantify the risks that an entity is who or what it claims to be during the authentication process. For example, as the consequence of an authentication error becomes more serious, the required level of authentication assurance should increase.</p>	
US 6	Risk vs. Control Objectives	New Clause	Te	Additional clarifying text. This is initial text that serves as an example of what could be included.	<p>Risk: Inaccurate information is recorded concerning an identity</p> <p>Control Objective: Limit those who can change and add identity data. Ensure checks made on data added to the identity record are accomplished in a manner that is equivalent to when the record was</p>	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.

Date: 2007-08-13	Document: SC27 N5875
------------------	-----------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
					created to include a review of the data before and after it is added.	
US 7						

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.



ISO/IEC JTC 1/SC 27 **N5875**

ISO/IEC JTC 1/SC 27/WG 5 **N55875**

REPLACES: N

ISO/IEC JTC 1/SC 27 Information technology - Security techniques Secretariat:
DIN, Germany

DOC TYPE: 1st Working Draft

TITLE: Text for ISO/IEC 1st WD 29115 – Information technology – Security techniques -- ~~Authentication assurance~~[Identity assurance](#)

SOURCE: Acting Editor

DATE: 2007-05-13

PROJECT: 29115

STATUS: This document was developed by the Acting Editor and approved at the SC 27 meeting held in Russia (May 2007).

As per Resolution 2 (contained in SC 27 N5939) of the 19th SC 27 Plenary meeting it is being circulated for study and comment by 2007-09-01.

ACTION ID: COM

DUE DATE: 2007-09-01

DISTRIBUTION:

P, O, L Members W. Fumy, SC 27 Chairman M. De Soete, SC 27 Vice Chair E. J. Humphreys, M.-C. Kang, K. Naemura, M. Ohlin, K. Rannenber WG-Conveners

MEDIUM: Livelink-server

NO OF PAGES: 1 + 5

Secretariat ISO/IEC JTC 1/SC27 DIN Deutsches Institut für Normung e.V., Burggrafenstrasse 6, 10787 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de [HTTP://www.ni.din.de/sc27](http://www.ni.din.de/sc27)

Scope

This standard provides objective and vendor neutral guidelines for identity assurance. It also describes

the guidelines or principles that must be considered in identity assurance and the rationale for why they are important to an authentication decision. The standard provides a framework for assessing "how close" an identity (individual) is to the correct one and provides guidelines for how the strength of the authentication can be measured. It also provides the basis for a set of identity assurance measures that are general and applicable to ~~a wide range of authentication mechanisms~~ the entire life cycle of an identity.

~~The goal of this standard is to identify a set of desirable guidelines for authentication metrics that take the following into account (see explanatory notes below):~~ The objective of this standard is to describe a set of guidelines that should be considered in assessing "how close" an identity is to the correct one throughout an identity's life cycle. This assessment takes into account the following:

- Authentication mechanisms
- Authentication protocols
- Characteristics of the device used to authenticate
- Location of the individual being authenticated
- Communications paths
- Relative ease of authentication manipulation by malicious behavior
- Corrections and modification of errors
- Identifier Types
- Identity Proofing
- Privacy

Introduction

Identity Assurance (IdA) involves technologies and processes to ensure that identity management (IdM) security controls are sufficient to make sure that an entity has confidence that the entity at the other end of an authentication transaction is who or what they say they are. IdA is the ability to associate identity attributes (email address, IP address, etc.) to an entity and the secure management and protection of this data. IdA is concerned with the proper risk associated with IdM to include the authentication process.

IdA consists of determining that an individual seeking a credential is who they say they are. Among other things, IdA involves the identity registration process. In order to determine that an individual seeking a credential is who they purport to be, it is necessary to first establish a history of identity by collecting identity information (e.g. biometric and biographical information). The next step is to validate the accuracy and legitimacy of the information collected and verifying the identity source documents. The final step in identity proofing is ensuring that identification credentials are provided only to correct individuals.

The goal of authentication assurance or Quality of Authentication (QoA) is to quantify the risks that an entity is who or what it claims to be during the authentication process. For example, as the consequence of an authentication error becomes more serious, the required level of authentication assurance should increase.

User authentication or authentication of individuals is a key security component of identity management. The goal of authentication assurance or Quality of Authentication (QoA) is to quantify the risks that an individual is not who or what he/she claims to be. Some measures used for assessing the level of assurance or confidence/risks for some authentication mechanisms already exist (cf. Bibliography).

The intent of this standard is to cover the three common methods for authentication:

- o Something you know, normally a password.
- o Something you have, normally a physical token.
- o Something you are, e.g. biometrics.

Criteria for authentication metrics are not widely agreed upon and those that do exist differ significantly. All identifiers used in authentication should not be treated equally or necessarily have the same authentication value. Metrics based on fundamental principles need to be assigned to each identifier in order to quantify the risk that an individual attempting to access IT resources is not the purported individual.

The resultant measured risk can then be provided to an access control service to grant, restrict, or deny access. In an authentication system based on metrics, information is provided by the individual, evaluated using metrics to calculate a score. The score is then used to determine whether the individual has provided correct information with sufficient accuracy to be authenticated.

Currently, an individual is authenticated or not based on a binary state in which an individual is deemed to match gets access and one who is deemed not to match is rejected. For example, a biometrics value may be deemed incorrect, but may have been off by only a small amount, or a password presented may not have been correct, but it may have differed from the correct one by some characteristic which could be easily explained by a typo or line lost. In this binary authentication process, there is no partial authentication or assessment of potential errors. One benefit of authentication assurance is that it allows for the authentication server to grant different levels of access, depending on the level of assurance achieved.

Without this proposed standard, organizations will find it difficult to assign objective and consistent values to the various components of authentication and as a result will find it difficult to make appropriate decisions about allowing access.

Criteria for authentication metrics

Authentication mechanism: It is generally accepted that static passwords are weaker than onetime password, and that a hardware token with a PIN is generally better than software token. However, there are no metrics to compare different types of biometrics authentication with each other or that compares biometrics authentication with hardware token-based authentication or public-key cryptography-based authentication. In order to assess authentication confidence, there needs to be standardized metrics to measure and determine the relative strength of the authentication method

Authentication protocol: A protocol that is known to be secure against man-in-the-middle attacks or one based on cryptographic operations is generally considered strong.

Characteristics of the device used to authenticate: Authentication assurance is partly based on the characteristics of the device being used by the user. For example, a COTS computer owned and controlled by the organization or a dedicated tamper resistant device is better than a publicly accessible COTS device.

Location of the entity being authenticated: One of the factors normally considered to be part of authentication assurance is the location of the user, e.g. within the organization's area or in public kiosk,

Internet Café, etc.. Authentication assurance will be higher if it is difficult for a public terminal in a kiosk to convince the authentication server that it is located within an organization's physical boundaries.

Communications path: Authentication typically involves a communications path (wireless networks, commercial leased lines, etc.) between the entity being authenticated and the server providing authentication and/or access decisions. In this scenario, authentication information must be reliably conveyed to the authentication server and it must not be susceptible to spoofing by an attacker.

Relative ease of authentication manipulation by malicious behavior: It is important to assess the risk associated with the compromise of cryptographic keys.

Corrections and modification of errors. For every type of authentication system, there are two types of errors. False positives are errors in which the wrong entity is authenticated as being the correct one and false negatives occurs when the correct entity is rejected. Each authentication can have its own set of false positives and negatives. For a password-based system a false positive occurs when an attacker knows the correct password whereas a false negative occurs when the legitimate use fails to enter the correct password--because it was forgotten or mistyped. For a false positive to occur the legitimate user's value is rejected as not matching the store value and the most sensitive information and resources will be withheld.

Identifier Type: The authentication value of an identifier depends on several factors including the issuer's relationship with the subject and the persistence of the identifier. An email address supplied by an employer is more strongly associated with an individual than one supplied by a paid ISP, which in turn is stronger than a throwaway from a free service such as gmail or yahoo.

Identity Proofing: In person registration and credential issuance is stronger than remote registration and delivery.

Privacy: Any static identifier has the potential to become personally identifiable information. Authentication systems should minimize a transmitted identifier's scope of applicability, lifetime, or both. An account number assigned for a single purpose is less sensitive than an SSN used for multiple purposes, and a onetime-use credit card number is less subject to misuse than a static credit card number.

Risk vs. Control Objectives

Risk: Inaccurate information is recorded concerning an identity.

Control Objective: Limit those who can change and add identity data. Ensure checks made on data to the identity record are accomplished in a manner that is equivalent to when the record was created to include a review of the data before and after it is added.

Definitions

cf. SD 6

Assurance: Activity resulting in a statement giving confidence that the authentication process fulfills specified requirements.

Authentication: Used definitions possibly to be taken into account, discussions on this needs to be continued:

the provision of assurance of the claimed identity of an entity

Provision of assurance of the claimed identity of an entity. [ISO/IEC 18028-4:2005]

the provision of assurance of the claimed identity of an entity. ([13])

the provision of assurance of the claimed identity of an entity. In case of user authentication, users are identified either by knowledge (e.g., password), by possession (e.g., token) or by a personal characteristic (biometrics). Strong authentication is either based on strong mechanisms (e.g., biometrics) or makes use of at least two of these factors (so-called multi-factor authentication).

assessing "how close" an identity (individual) is to the correct one (rf. Scope, above)

Assurance Level: The amount of assurance obtained according to the specific scale used by the assurance method. NOTE 1. the assurance level may not be measurable in quantitative terms. NOTE 2. The amount of assurance obtained is generally related to the effort expended on the activities performed.

Bibliography

In the area of electronic authentication (E-Authentication) there are two U.S. Government documents that establish and describe four levels of identity assurance for electronic transactions requiring authentication and also provide useful QoA information:

- *OMB M-04-04, E-Authentication Guidance for Federal Agencies*

<http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>

- *NIST SP800-63, Electronic Authentication Guideline*

http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

In the area of biometrics and E-Authentication, there is a U.S. INCITS M1 draft report that explains how biometrics should be used in the four assurance levels defined in OMB M04-04 and NIST SP 800-63:

- *Study Report on Biometrics in E-Authentication*

http://www.incits.org/tc_home/m1htm/2006docs/m1060642.pdf

The above documents are narrowly focused with respect to this proposal since E-Authentication is a subset of authentication for physical and logical access control. Also, the U.S. INCITS M1 draft study focuses on only on biometrics.

- New Zealand Standard: Evidence of Identity (EOI) (URL will follow)

Information technology — Security techniques — Identity Assurance

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

Copyright notice

This ISO document is a working draft or committee draft and is copyright-protected by ISO. While the reproduction of working drafts or committee drafts in any form for use by participants in the ISO standards development process is permitted without prior permission from ISO, neither this document nor any extract from it may be reproduced, stored or transmitted in any form for any other purpose without prior written permission from ISO.

Requests for permission to reproduce this document for the purpose of selling it should be addressed as shown below or to ISO's member body in the country of the requester:

[Indicate the full address, telephone number, fax number, telex number, and electronic mail address, as appropriate, of the Copyright Manger of the ISO member body responsible for the secretariat of the TC or SC within the framework of which the working document has been prepared.]

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

Contents

Page

Foreword	iv
Introduction.....	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
3.1 Assurance	2
3.2 Authentication	2
3.3 Assurance Level	2
4 Symbols (and abbreviated terms)	2
5 Criteria for authentication metrics	2
5.1 Authentication mechanism	2
5.2 Authentication protocol	3
5.3 Characteristics of the device used to authenticate	3
5.4 Location of the entity being authenticated	3
5.5 Communications path	3
5.6 Relative ease of authentication manipulation by malicious behavior	3
5.7 Corrections and modification of errors	3
5.8 Identifier Type	3
5.9 Identity Proofing	4
5.10 Privacy	4
6 Risk vs. Control Objectives	4
Bibliography.....	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 29115 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Joint Technical Committee, Subcommittee SC 27, Information technology - Security techniques*.

This second/third/... edition cancels and replaces the first/second/... edition (), [clause(s) / subclause(s) / table(s) / figure(s) / annex(es)] of which [has / have] been technically revised.

Introduction

Identity Assurance (IdA) involves technologies and processes to ensure that identity management (IdM) security controls are sufficient to make sure that an entity has confidence that the entity at the other end of an authentication transaction is who or what they say they are. IdA is the ability to associate identity attributes (email address, IP address, etc.) to an entity and the secure management and protection of this data. IdA is concerned with the proper risk associated with IdM to include the authentication process.

IdA consists of determining that an individual seeking a credential is who they say they are. Among other things, IdA involves the identity registration process. In order to determine that an individual seeking a credential is who they purport to be, it is necessary to first establish a history of identity by collecting identity information (e.g. biometric and biographical information). The next step is to validate the accuracy and legitimacy of the information collected and verifying the identity source documents. The final step in identity proofing is ensuring that identification credentials are provided only to correct individuals.

The goal of authentication assurance or Quality of Authentication (QoA) is to quantify the risks that an entity is who or what it claims to be during the authentication process. For example, as the consequence of an authentication error becomes more serious, the required level of authentication assurance should increase.

User authentication or authentication of individuals is a key security component of identity management. The goal of authentication assurance or Quality of Authentication (QoA) is to quantify the risks that an individual is not who or what he/she claims to be. Some measures used for assessing the level of assurance or confidence/risks for some authentication mechanisms already exist (cf. Bibliography).

The intent of this standard is to cover the three common methods for authentication:

- Something you know, normally a password.
- Something you have, normally a physical token.
- Something you are, e.g. biometrics.

Criteria for authentication metrics are not widely agreed upon and those that do exist differ significantly. All identifiers used in authentication should not be treated equally or necessarily have the same authentication value. Metrics based on fundamental principles need to be assigned to each identifier in order to quantify the risk that an individual attempting to access IT resources is not the purported individual.

The resultant measured risk can then be provided to an access control service to grant, restrict, or deny access. In an authentication system based on metrics, information is provided by the

individual, evaluated using metrics to calculate a score. The score is then used to determine whether the individual has provided correct information with sufficient accuracy to be authenticated.

Currently, an individual is authenticated or not based on a binary state in which an individual is deemed to match gets access and one who is deemed not to match is rejected. For example, a biometrics value may be deemed incorrect, but may have been off by only a small amount, or a password presented may not have been correct, but it may have differed from the correct one by some characteristic which could be easily explained by a typo or line lost. In this binary authentication process, there is no partial authentication or assessment of potential errors. One benefit of authentication assurance is that it allows for the authentication server to grant different levels of access, depending on the level of assurance achieved.

Without this proposed standard, organizations will find it difficult to assign objective and consistent values to the various components of authentication and as a result will find it difficult to make appropriate decisions about allowing access.

Information technology — Security techniques — Identity Assurance

1 Scope

This standard provides objective and vendor neutral guidelines for identity assurance, It also describes the guidelines or principles that must be considered in identity assurance and the rationale for why they are important to an authentication decision. The standard provides a framework for assessing "how close" an identity (individual) is to the correct one and provides guidelines for how the strength of the authentication can be measured. It also provides the basis for a set of identity assurance measures that are general and applicable to the entire life cycle of an identity.

The goal of this standard is to identify a set of desirable guidelines for authentication metrics that take the following into account (see explanatory notes below):

- Authentication mechanisms
- Authentication protocols
- Characteristics of the device used to authenticate
- Location of the individual being authenticated
- Communications paths
- Relative ease of authentication manipulation by malicious behavior
- Corrections and modification of errors
- Identifier Types
- Identity Proofing
- Privacy

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.

ISO ab-c:199x, General title of series of parts — Part c: Title of part

ISO xyz (all parts), General title of the series of parts

3 Terms and definitions

For the purposes of this document, **the following terms and definitions apply / the terms and definitions given in ... and the following apply.**

cf. SD 6

3.1 Assurance

Activity resulting in a statement giving confidence that the authentication process fulfills specified requirements.

3.2 Authentication

Used definitions possibly to be taken into account, discussions on this needs to be continued:

- Provision of assurance of the claimed identity of an entity
- Provision of assurance of the claimed identity of an entity. [ISO/IEC 18028-4:2005]
- Provision of assurance of the claimed identity of an entity. ([13])
- Provision of assurance of the claimed identity of an entity. In case of user authentication, users are identified either by knowledge (e.g., password), by possession (e.g., token) or by a personal characteristic (biometrics). Strong authentication is either based on strong mechanisms (e.g., biometrics) or makes use of at least two of these factors (so-called multi-factor authentication).
- assessing "how close" an identity (individual) is to the correct one (rf. Scope, above)

3.3 Assurance Level

The amount of assurance obtained according to the specific scale used by the assurance method. NOTE 1. The assurance level may not be measurable in quantitative terms. NOTE 2. The amount of assurance obtained is generally related to the effort expended on the activities performed.

4 Symbols (and abbreviated terms)

A paragraph.

5 Criteria for authentication metrics

5.1 Authentication mechanism

It is generally accepted that static passwords are weaker than onetime password, and that a hardware token with a PIN is generally better than software token. However, there are no metrics to compares different types of biometrics authentication with each other or that compares biometrics authentication with hardware token-based authentication or public-key cryptography-based authentication. In order to assess authentication confidence, there needs

to be standardized metrics to measure and determine the relative strength of the authentication method.

5.2 Authentication protocol

A protocol that is known to be secure against man-in-the-middle attacks or one based on cryptographic operations is generally considered strong.

5.3 Characteristics of the device used to authenticate

Authentication assurance is partly based on the characteristics of the device being used by the user. For example, a COTS computer owned and controlled by the organization or a dedicated tamper resistant device is better than a publicly accessible COTS device.

5.4 Location of the entity being authenticated

One of the factors normally considered to be part of authentication assurance is the location of the user, e.g. within the organization's area or in public kiosk, Internet Café, etc.. Authentication assurance will be higher if it is difficult for a public terminal in a kiosk to convince the authentication server that it is located within an organization's physical boundaries.

5.5 Communications path

Authentication typically involves a communications path (wireless networks, commercial leased lines, etc.) between the entity being authenticated and the server providing authentication and/or access decisions. In this scenario, authentication information must be reliably conveyed to the authentication server and it must not be susceptible to spoofing by an attacker.

5.6 Relative ease of authentication manipulation by malicious behavior

It is important to assess the risk associated with the compromise of cryptographic keys.

5.7 Corrections and modification of errors

For every type of authentication system, there are two types of errors. False positives are errors in which the wrong entity is authenticated as being the correct one and false negatives occurs when the correct entity is rejected. Each authentication can have its own set of false positives and negatives. For a password-based system a false positive occurs when an attacker knows the correct password whereas a false negative occurs when the legitimate user fails to enter the correct password--because it was forgotten or mistyped. For a false positive to occur the legitimate user's value is rejected as not matching the stored value and the most sensitive information and resources will be withheld.

5.8 Identifier Type

The authentication value of an identifier depends on several factors including the issuer's relationship with the subject and the persistence of the identifier. An email address supplied by an employer is more strongly associated with an individual than one supplied by a paid ISP, which in turn is stronger than a throwaway from a free service such as gmail or yahoo.

5.9 Identity Proofing

In person registration and credential issuance is stronger than remote registration and delivery.

5.10 Privacy

Any static identifier has the potential to become personally identifiable information. Authentication systems should minimize a transmitted identifier's scope of applicability, lifetime, or both. An account number assigned for a single purpose is less sensitive than an SSN used for multiple purposes, and a onetime-use credit card number is less subject to misuse than a static credit card number.

6 Risk vs. Control Objectives

Risk: Inaccurate information is recorded concerning an identity.

Control Objective: Limit those who can change and add identity data. Ensure checks made on data added to the identity record are accomplished in a manner that is equivalent to when the record was created to include a review of the data before and after it is added.

Bibliography

Note: In the area of electronic authentication (E-Authentication) there are two U.S. Government documents that establish and describe four levels of identity assurance for electronic transactions requiring authentication and also provide useful QoA information:

[1] OMBM-04-04, *e-Authentication Guidance for Federal Agencies*
<http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>

[2] NISTSP800-63, *Electronic Authentication guideline*
http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

In the area of biometrics and E-Authentication, there is a U.S. INCITS M1 draft report that explains how biometrics should be used in the four assurance levels defined in OMB M04-04 and NIST SP 800-63:

[3] *Study Report on Biometrics in E-Authentication*
http://www.incits.org/tc_home/m1htm/2006docs/m1060642.pdf

The above documents are narrowly focused with respect to this proposal since E-Authentication is a subset of authentication for physical and logical access control. Also, the U.S. INCITS M1 draft study focuses on only on biometrics.

[4] New Zealand Standard: *Evidence of Identity (EOI)* (URL will follow)