

CS1/06-0186 US National Body Contribution on 1st WD 24760
 [MB¹] NB comments on 1st WD 24760

Date: 2006-03-DD	Document: SC27 N5205
------------------	----------------------

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
	General		ge	This is an excellent first Working Draft. It is apparent that the Identity Management Study Group accomplished a lot in a very short period of time. The document has a lot of merit and will be an excellent standard. However, there are several areas that need further inputs and the comments that follow are an attempt to accomplish this objective.		
US-1	General			<p>A lot of the information is very abstract for a standard. Practical examples of identity management should be inserted where possible. Some are provided in the following comments.</p> <p>The title is Identity Management Framework. However, the components of Identity Management are not discussed until Clause 8.3, p.11. Furthermore, what is normally considered as the components of an identity management framework are included in Clause 9.2 Role based access control, 9.3 Provisioning, 9.4.5 Digital Certificates, 9.5 Single Sign-On, and 10.1 Directories. Furthermore, there is no discussion of PKI.</p>	<p>Re-assemble the existing text in a manner that includes all the major components of an identity management framework into a Clause that is called "Framework Components. Include in this new Clause a subclause called "Public Key Infrastructure" that includes the following text:</p> <p>Public Key Infrastructure (PKI)</p> <p>An infrastructure that enables applications to utilize the digital authentication and authorization capabilities that it provides.</p>	
US-2	All	All	Ge	The document is not exact and consistent in its choice and use of terms. New terms are introduced to describe concepts that have already been associated with an existing term. The loose language creates vagueness and makes it unnecessarily difficult to comprehend the intricate facets of the framework. Specific examples are provided in the comments below.		
US-3	All	All	Ed	All uses of "e.g." should be followed by a comma.	Search on "e.g." and replace with "e.g.,"	
US-4	1	2 nd paragraph	Te	Identity management is rather poorly defined and the document assumes the reader understands Identity Management if (s)he has an understanding of the	The proposal is to incorporate a more descriptive definition of Identity Management. We offer the following	

Comment [s1]:

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.

CS1/06-0186 US National Body Contribution on 1st WD 24760

[MB¹] NB comments on 1st WD 24760

Date: 2006-03-DD	Document: SC27 N5205
------------------	-----------------------------

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 com- ment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
				independent terms "identity" and "management." In fact, the document defines Identity Management by using its component terms. For example, paragraph 2 of Section 1 states "Identity Management (IdM) is the secure management of identities, . . ."	definition for Identity management: Identity Management is an integrated system of business processes, policies and technologies that enable organizations to facilitate and control their users' access to critical online applications and resources — while protecting confidential personal and business information from unauthorized users. It represents a category of interrelated solutions that are employed to administer user authentication, access rights, access restrictions, account profiles, passwords, and other attributes supportive of users' roles/profiles on one or more applications or systems.	
US-5	1	3 rd paragraph	Te	The term "context" is used throughout the document without first defining it in the standard text. A definition is provided in the Terms and Definitions section. The first appearance of the word context is in Section 1.	Begin paragraph 3 with the following sentence: "The context of an identity is the environment in which an entity exists and is recognized by an authoritative source."	
US-6	1.2	1 st and 2nd paragraphs	Ed	For clarification move 1 st Para of existing Clause 1.0 and additional text to a new clause 1.1 Purpose according to the proposed change.	1.0 Introduction 1.1 Purpose This standard defines identity, explains the underlying concepts for identity management and provides a framework for secure reliable, and management of identity information. This framework should be applicable to individuals as well as organizations of all types and sizes, in any environment and regardless of the nature of the activities	

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.

CS1/06-0186 US National Body Contribution on 1st WD 24760
[MB¹] NB comments on 1st WD 24760

Date: 2006-03-DD	Document: SC27 N5205
------------------	-----------------------------

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 com- ment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
					they are involved in. 1.2 Scope Identity management (IDM) May be used in different contexts.	
US-7	1.2	6 th paragraph	Ed	For clarification, add the following text at the end of the 1 st sentence.	For example, it is a key security component for international emergency and disaster relief activities where strong authentication of users, devices, processes and communications is prerequisite for authorizing access to available resources.	
US-8	1.2,	5 th paragraph	Ed	For clarification, add the following text at the end of the sentence.	"i.e., human resource database, user profiles in telecommunications networks."	
US-9	3	N/A	Ed	The term Identity Registrar, which is used to explain identity proofing, is not defined itself	Define Identity Registrar in Section 3 (Terms and Definitions).	
US-10	5.3	1 st and 2 nd paragraphs	Te	The relationships between entity, identity, attributes, context, and identity reference do not come across clearly in the text alone.	Suggest adding a figure in this section to illustrate the notion that there is a one-to-many relationship between an entity and its identities and that each identity can have several attributes. It is further suggested to illustrate the concept that an entity can have multiple identity references in each context.	
US-11	5.4	4 th paragraph	Ed	Modify "The identification process helps providing the entity with. . . ."	Change to "The identification process provides the entity with. . . ."	
US-12	5.4	ALL	Te	The terms "characteristics" and "attributes" appear to be used interchangeably in throughout the document.	If they are meant to be congruent, then select one term and use it consistently. Otherwise, define the difference between them and use each carefully.	

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.

CS1/06-0186 US National Body Contribution on 1st WD 24760
[MB¹] NB comments on 1st WD 24760

Date: 2006-03-DD	Document: SC27 N5205
------------------	-----------------------------

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 com- ment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
US-13	5.5	1 st paragraph	Te	The notion of "context" is further described in this section. It then extends the idea of context to "multiple domains of applicability" but does not define what is meant by a domain and how it differs from a context.	Describe the concept of a "domain" and its relationship to "context." Illustrate it in a figure, if possible.	
US-14	5.6	3 rd paragraph	Ed	Modify "Consequently,, different sets of characteristics. . ."	Remove extra comma. Change to "Consequently, different sets of characteristics. . ."	
US-15	5.7	1 st paragraph	Te	The term "context" is further defined in this paragraph. It states that "contexts are delimited by boundaries of applicability" and later states that "Contexts apply to a number of domains of activities that can be described as domains of applicability . . ."	If the phrase "boundaries of applicability" is meant to be synonymous with "domains of applicability," then select one term and use it consistently. Otherwise, define the difference between them and use each carefully. If a context is delimited by boundaries of applicability, is the notion of a context the same as a domain of applicability? The difference is not clear. If there is a difference, it needs to be clearly described and the definition of context and its first use in Section 1 should be updated to include the concept of domains of applicability. Otherwise, the use of both may be unnecessary.	
US-16	5.7	2 nd paragraph	Ed	Modify "In the late example, it is obvious that the person. . ."	Change to "In the latter example, it is obvious that the person. . ."	
US-17	5.7	2 nd paragraph	Ed	Modify This could ends in issues where privileges . . ."	Change to "This could result in issues where privileges . . ."	
US-18	5.7	2 nd paragraph	Ed	(Same sentence as immediately above) Modify "process refer to"	Change "process refer to" to "process refers to" or "processes refer to" whichever make most sense to the author	

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.

CS1/06-0186 US National Body Contribution on 1st WD 24760
 [MB¹] NB comments on 1st WD 24760

Date: 2006-03-DD	Document: SC27 N5205
------------------	-----------------------------

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 com- ment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
US-19	5.9	1 st paragraph	Ed	The expression "may as well" seems very casual. Modify "Entities may as well decide to keep..."	Consider the following instead: "Alternatively, entities may decide to keep..."	
US-20	5.10	1 st paragraph	Ed	Modify "The sharing of entity's attributes between contexts . . ."	Change to "The sharing of an entity's attributes between contexts . . ."	
US-21	5.10	2 nd paragraph	Ed	Add colon at end of sentence.	Change to "Specifically, identity management solutions require minimum common controls of : "	
US-22	5.11	2 nd paragraph	Te	The term "entity is profile" is used both in the figure and subsequent text without defining it. The reader is to assume the profile contains a list of attributes about the entity. However, the text is loose and not exact and describes the profile as a "list of useful information on the entity."	Define the term "entity profile" and be consistent in the use of terms, such as using the term "attributes" instead of "information," if this is the intended meaning.	
US-23	5.11	Figure	Te	Why is the entity included in the context box? Up to this point, the standard suggests that the entity exists outside the context. The entity identity is what exists in the each context. The figure suggests by placing the entity in each of two contexts that an entity is not necessarily unique.		
US-24	5.11	3 rd paragraph	Te	What are the significance of an "IT" entity and an "IT domain of applicability? How is it different from an entity and domain of applicability as previously used in the document? Is this meant to be a specific example? If so, it must be stated.	Resolve the meaning and purpose of "IT entity" and "IT domain of applicability."	
US-25	5.11	Figure	Te	The figure illustrates the existence of entity profiles and entity identities that can exist outside of the context construct. They appear to exist in a domain of applicability. The reader was lead to believe that entity identities must always exist in a context. Section 5.7 states that context's are delimited by "boundaries of applicability." How is this shown in the figure? The figure	Make the figure consistent with the standard 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.

CS1/06-0186 US National Body Contribution on 1st WD 24760

[MB¹] NB comments on 1st WD 24760

Date: 2006-03-DD	Document: SC27 N5205
------------------	-----------------------------

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
				seems to create confusion with the standard text.		
US-26	6	1 st paragraph	Ed	Modify "This is an important step without what the entity . . ."	Change to "This is an important step without which the entity. . ."	
US-27	6.1	1 st paragraph	Te	For clarification, add the following text at the end of the sentence.	Identity management provides the capability to cryptographically bind and authenticate users and physical devices through the use of public key and a public key infrastructure. It replaces today's multiple on-line, easy to steal, crack, misuse or guess passwords (single factor authentication) with secure, trusted, and efficiently managed digital credential (X509 Certificates). It provides the capability to understand how, when and by whom network resources are being accessed.	
US-28	6.2	2 nd paragraph	Ed	In this paragraph, the author provides a good example to the statement "Some entity associations might be formal, specific relationships..." However, the next statement which talks about "Other associations might be informal, loosely-linked, one-to-many and many-to-many affiliations..." does not have an example, and leaves the reader wondering.	Consider providing an example of one-to-many or many-to-many affiliations, to remain consistent with the previous sentence in that paragraph.	
US-29	6.2.2.1	1 st paragraph	Ed	(Last sentence in paragraph) Modify "Requirements are generally based on the sensitivities of the privileges granted in relation with to the entity."	Change "with to" to either "with" or "to" (not both)	
US-30	6.2.2.3	2 nd and 3 rd paragraph	Ed	This information is not specific to "mutual authentication." Little in this section actually describes the role and purpose of mutual authentication.	Move information to the introduction section or delete. Expand on the role and purpose of mutual authentication.	
US-31	6.2.3	1 st paragraph	Ed	Modify "Binding identities with attributes is the process . . ."	Change to "Binding attributes to identities is the process . . ."	

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.

CS1/06-0186 US National Body Contribution on 1st WD 24760
[MB¹] NB comments on 1st WD 24760

Date: 2006-03-DD	Document: SC27 N5205
------------------	-----------------------------

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-32	6.2.5	1 st paragraph	Ed	Modify "Authoritative Sources sees..."	Change to "Authoritative Source sees...."	
US-33	6.2.6	1 st paragraph	Ed	Modify "a relation between an entity's identify..."	Change to "a relation between an entity's identity..."	
US-34	8.1	2 nd paragraph	Ed	(Second Sentence) Modify "which has implemented an identity management."	Change to "which has implemented an identity management system (IdMS)."	
US-35	8.1	3 rd paragraph	Ed	Need a colon. Modify "An iDMS provides"	Change to ""An iDMS provides:""	
US-36	8.3	1 st paragraph	Ed	Modify "(IdMS) must provide accurate and updated information on entities, potential users"	Change to "(IdMS) must provide accurate and updated information on entities, and potential users"	
US-37	8.3	3 rd paragraph	Ed	(Second Sentence) Modify "the IdM controls"	Change to "the IdMS controls"	
US-38	8.3	3 rd paragraph	Ed	Need to define the acronym "IdS" used in the figure	Change "A central store, the Identity Store, collects . . ." to "A central store, the Identity Store (IdS), collects . . ."	
US-39	8.3	3 rd paragraph	Ed	IDS is a widely accepted term used in the information security industry, and refers to Intrusion Detection Systems.	Consider changing "IdS" in this document to another acronym such as "IdStore"	
US-40	8.3.4	1 st paragraph	Ed	(Fourth Sentence) Modify "The IdMS must also be seen as another An AS can act on behalf..."	Consider changing to "The IdMS must also be seen as another AS. An AS can act on behalf..."	
US-41	9.1	2 nd paragraph	Ed	Modify "An Identity Management framework is the primarily stone to an efficient security access. . ."	Change to "An Identity Management framework is the foundation of an efficient security access . . ."	
US-42	9.3.2.6		Te	Add the following new Clause	9.3.2.6 Delegated Authority Under certain conditions, an identity may legitimately be required to take on	

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.

CS1/06-0186 US National Body Contribution on 1st WD 24760
[MB¹] NB comments on 1st WD 24760

Date: 2006-03-DD	Document: SC27 N5205
------------------	-----------------------------

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 com- ment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
					the identity of another in a particular role. For instance, standing in for the boss who is away on vacation	
US-43	9.3.2.2		Te	Insert the following text at the end of the first sentence	For example, people on the move can play a different role within different environments i.e. privileges in one environment may be valueless in another environment.	
US-44	9.4.5		Te	Insert the following text where none exist.	A digital certificate is an electronic file used in public key cryptography that binds information about an identity with the identity's public key. It is used for authentication of individuals, service, and devices. It is also known as a PKI Certificate or an X.509 Digital Certificate.	
US-45	9.5		Te	Insert the following text where none exist.	Traditionally identity has been done in a static way that greatly limits flexibility. It is typically associated with static, multiple, easy to steal, crack, misuse or guess single factor identity authentication techniques (username and passwords). This type of identity mechanism should be replaced with a single, secure, trusted and efficiently managed digital credential such as X.509 Certificates. This single sign-on (SSO) capability allows a user to sign in once to claim their privileges to all applications and data residing on the network. In other words, SSO is the ability of a user to authenticate once to a single authentication authority, obtain a credential token, and use it to access	

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.

CS1/06-0186 US National Body Contribution on 1st WD 24760
 [MB¹] NB comments on 1st WD 24760

Date: 2006-03-DD	Document: SC27 N5205
------------------	-----------------------------

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 com- ment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
					protected resources without re-authentication. The SSO identity mechanism allows a user free movement among multiple domains and applications. It will also significantly reduce the number of logons by a user and consequently the number of potential entry points for network attackers.	
US-46	9.6 or 5.8		Te	Add the following new Clause or insert in 5.8	<p>9.6 Federation and Interoperability</p> <p>The sharing of identification credentials among several organizations is essential. Identity Interoperability or federation is accomplished when trust is transferred from one identifying and authenticating organization to another. However, the identity information held by one organization is generally not consumable by another organization. Federated identities address this interoperability issue among identity management mechanisms.</p> <p>Federation of identity management mechanisms allows organizations to share trusted identities across the boundaries that separate them. Consequently, organizations should ensure that its identity management mechanisms can be federated with other organizations and should avoid isolated identity management systems. In other words, issuing organization credentials that are capable of operating in a federated identity management</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.

CS1/06-0186 US National Body Contribution on 1st WD 24760
[MB¹] NB comments on 1st WD 24760

Date: 2006-03-DD	Document: SC27 N5205
------------------	-----------------------------

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 com- ment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
					environment will greatly improve an organization's identity management capabilities.	
US-47	10.1		Te	Directories are a major component of the identity Management Framework and Directories should be included in Clause 9.	Merge Clause 10.1 with Clause 9 by re-labelling it as 9.x	
US-48	10.1		Te	Insert the following text at the end of paragraph	The information stored in the directories is very sensitive. Based on a risk assessment, appropriate security controls need to be put in place to protect the directory data.	
US-49	Annex		Te	An Annex is needed to explain what new IdM projects should be undertaken by WG5	See the attached proposed projects.	
US-50	6.2.2.3	3	ge	add to first sentence	add “, although US banks are moving to two-factor authentication by the end of 2006 to meet regulatory requirements.”	
US-51	9.2	1	ge	add after 1 st sentence	Many commercial RBAC products allow the specification of rules as constraints. Rules can also be used with the XACML RBAC standard.	
US-52	9.2	1	ge	Should clarify that you are not saying the rule based system should conform to core RBAC. Also note that core RBAC does not include constraints, which is where rules come in to RBAC. It may be best to leave out mention of rule based systems here and address that idea in a separate place.	drop discussion of rule based systems in this section	
US-53	9.2	1	ed	wording	remove “while” in sentence beginning “Organizations that rely...”	
US-54	9.1		ge	Initiatives such as OATH have demonstrated the need for authentication frameworks that are flexible in multiple	* Efficient and flexible authentication management	

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.

CS1/06-0186 US National Body Contribution on 1st WD 24760
[MB¹] NB comments on 1st WD 24760

Date: 2006-03-DD	Document: SC27 N5205
------------------	-----------------------------

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 com- ment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
				ways (e.g., form factors and mechanisms).		
US -55	10.1.2		ge	It's unclear why attribute certificates (ACs) are called out as an approach to handling attributes associated with identities. IdM isn't limited to public key technology.	Provide the rationale for calling out ACs.	

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: 2006-03-DD	Document: SC27 N5205
------------------	-----------------------------

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 com- ment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

Annex A

Additional IdM Work Item Proposals (or potential topics to incorporate in the IdM framework document):

1. **Security Framework/Reference Architecture for IdM Systems:** Identity management systems will contain information that attackers will seek to obtain or modify. Identity management systems will therefore be a target of malicious attacks. This is a proposal for the standards group to develop a security framework and/or reference architecture for identity management systems, to identify the security threats and risks, and to provide some guidance on the security measures that are needed to protect the different elements of identity management systems. Proposed standard N5205 describes the components of an identity management system in section 8.3, but it does not address its security. For instance, what security measures are prudent to track changes, support auditing/forensic capabilities, or detect fraud? What security measures, for instance, mutual authentication, confidentiality and integrity protection of information transfer, are needed for different identity management systems to exchange information with each other? What are the security issues with maintaining high availability of identity management systems? Will a targeted DoS attack, for instance, on an identity management system effectively deny all system access? Can an identity management system be poisoned and can it be used to propagate invalid or rogue information? How is this scenario to be prevented?
2. **Framework for Interactions between Multiple Identity Management Domains:** Identity management is often considered in the scope of a single domain, such as an enterprise domain where identity information for the organization's employees is managed. But its applicability extends well beyond single domains and many applications, such as government and management of citizen identity data, requires interactions between identity management systems at all levels. This is a proposal for the standards group to develop a framework on how identity management systems can exchange information across multiple domains, whether it be in an enterprise or government (local or national) environment. This proposal would build upon the privacy framework (N5211), the reference architecture (N5212), and the identity management framework (N5205). Section 5.3 in N5205 briefly touches upon the notion that uniqueness must be maintained across identity management systems and a global identity reference supports this need. Is there a recommended strategy to create global identity references? How should conflicts be resolved? What other issues are there with multi-domain identity management? Should there be a framework for the formation of the federations that are described in Section 5.8 of N5205?

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: 2006-03-DD	Document: SC27 N5205
------------------	-----------------------------

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 com- ment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

3. **Role-Based Access Control Standardization for Management of Critical Communications Infrastructures:** The secure management and operation of the telecommunications infrastructure is arguably a priority for the U.S. Government and for Governments around the world as well as are the communications systems used in other critical infrastructures (i.e., power via SCADA systems). The Operations, Administration, Maintenance and Provisioning functions are well known and established disciplines. Operations encompass automatic monitoring of the network environment, which includes detecting, correlating, and performing root-cause analysis of alarms, faults, and security events. Administration typically involves collecting performance statistics, accounting data for the purpose of billing, capacity planning using usage data, and maintaining system reliability. It can also involve maintaining the service databases that are used to determine periodic billing. Maintenance involves upgrades, fixes, new feature enablement, backup and restore functions, and monitoring the network health. The major task of maintenance is diagnostics and troubleshooting. Provisioning is the setting up of the user accounts, devices, and services. There are many types of interactions that take place within the OAM&P framework: human-to-machine (including remote access), computer-to-computer, process-to-process, network-to-network, etc. This is a proposal for the standards group to investigate and develop detailed role-based access control profiles for entities (people, devices) used to manage critical communications infrastructures and network elements / equipment within the identity management framework.
4. **Password Synchronization Capabilities:** Password synchronization is a capability to maintain a common password across multiple user objects and systems and is subject to common security policies. In some circles, password synchronization is considered an identity management capability that is more effective at managing password problems than single sign-on capabilities. For instance, there is no single point of failure in password synchronization. This is a proposal for the standards group to provide some guidance on the use of password synchronization as part of identity management and investigate the most appropriate use of both single sign-on and password synchronization capabilities. Are there situations where single sign-on is more appropriate to use than password synchronization and vice versa? What are the security vulnerabilities and risks for each? What types of single sign-on and password synchronization methods exist? For instance, two common types of password synchronization are the automatic and manual approaches. In the automatic approach, the new password is automatically propagated to the user's other objects or systems based on a password update. In the manual method, the user takes an action specifically to synchronize passwords, such as access a Web-based capability. At minimum, mention of this capability in the N5205 identity management framework is advised.
5. **Single Sign-out Capability:** Single sign-out is the converse of single sign-on. If a user logs out of one session or account, the user is automatically logged out of all sessions and accounts. This is a proposal for the standards group to investigate the use, appropriateness, and issues with using single sign-out capabilities as part of identity management and provide guidance on the use single sign-out capability in the identity management framework. At minimum, mention of this capability in the N5205 identity management framework is advised.

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.

CS1/06-0186 US National Body Contribution on 1st WD 24760
 [MB¹] NB comments on 1st WD 24760

Date: 2006-03-DD	Document: SC27 N5205
------------------	-----------------------------

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 com- ment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment

6. **Support for Network Segregation Technologies (e.g., Virtual Local Area Networks -VLANs):** Segregation of traffic using VLANs is a growing method of isolating trusted and untrusted traffic, VoIP from data traffic, management traffic from user traffic, internal and business partner traffic, possibly signaling and media traffic. VLANs will be used extensively as a security measure in NGNs and enterprise networks. This is a proposal for the standards group to investigate whether identify management systems need to incorporate any special functional capabilities to specifically support VLAN segregation.

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.