

M1/06-0127

Title: BIAS – base document contribution

Source: Daon (project co-sponsor), Purdue University

Date: February 7, 2006

Comments: For discussion at February 21, 2006 meeting of M1.2

References: M1/05-0789, M1/05-0830, M1/05-0882

Contents

1	Scope	6
2	Conformance	6
3	Normative References	6
4	Terms and Definitions.....	7
5	Symbols and Abbreviated Terms.....	7
6	System Context	7
6.1	Service Oriented Architectures	7
6.2	BIAS Architecture	9
6.3	BIAS Requirements	10
7	Biometric Services.....	11
7.1	Primitive Services	11
7.1.1	Add Subject to Gallery	11
7.1.2	Check Background	11
7.1.3	Check Quality	11
7.1.4	Classify Biometric Data	12
7.1.5	Create Subject.....	12
7.1.6	Delete Biographic Data.....	12
7.1.7	Delete Biometric Data.....	13
7.1.8	Delete Subject	13
7.1.9	Delete Subject From Gallery	13
7.1.10	Identify Subject.....	14
7.1.11	List Biographic Data	14
7.1.12	List Biometric Data	14
7.1.13	Perform Fusion	15
7.1.14	Retrieve Biographic Information	15
7.1.15	Retrieve Biographic Information	15
7.1.16	Set Biographic Data.....	16
7.1.17	Set Biometric Data.....	16
7.1.18	Transform Biometric Data.....	17
7.1.19	Update Biographic Data	17
7.1.20	Update Biometric Data	18
7.1.21	Verify Subject	18
7.2	Aggregate Services	18
7.2.1	Enroll	19
7.2.2	Identify.....	19
7.2.3	Retrieve Information	20
7.2.4	Verify	20
8	Data Elements	21
9	Error Handling and Notification.....	21

10 Security22

Foreword

INCITS (The International Committee for Information Technology Standards) is the ANSI recognized Standards Development Organization for information technology within the United States of America. Members of INCITS are drawn from Government, Corporations, Academia and other organizations with a material interest in the work of INCITS and its Technical Committees. INCITS does not restrict membership and attracts participants in its technical work from 13 different countries, and operates under the rules of the American National Standards Institute.

In the field of Biometrics, INCITS has established the Technical Committee M1. Standards developed by this Technical Committee have reached consensus throughout the development process and have been thoroughly reviewed through several Public Review processes. In addition, the INCITS Executive Board and the ANSI Board of Standards Review have approved this American National Standard for Publication as an INCITS Standard.

(Patent Statement to be inserted at this point)

Introduction

Biometric technologies are being used today in a wide variety of applications and environments. At the same time, enterprises – both commercial and government – have been moving towards services-based architectures as the framework for their enterprise infrastructures. As biometrics become a larger part of the greater identity assurance capability, the need to access these services remotely across those services-oriented frameworks will become necessary. Indeed, the ability to do so in a standardized way is already a need.

A current gap exists in standards related to the use of biometric technology in a services oriented architecture (SOA). The Biometric Identity Assurance Services (BIAS) standard is intended to fill that gap by defining a framework for deploying and invoking biometrics-based identity assurance capabilities that can be readily accessed using services-based frameworks (e.g. web services).

The BIAS standard will help ensure biometric-based solutions are robust and maintainable, while providing a mechanism for accessing an organization's biometric services.

This standard is intended to provide a service-based framework for delivering identity assurance capabilities, allowing for platform and application independence. The standard is intended to have the following characteristics:

- Focused on biometrics (though not exclusively)
- Biometric device, type, and vendor independent
- Leverage existing standards where appropriate (e.g. CBEFF – INCITS 398-2005).
- Transport mechanism independent (OASIS will provide bindings for Web services in a separate standard)
- Multi-platform, open
- Primarily focused on remote invocations (services), i.e. not dealing with local devices

The benefits of implementing such a standard are:

- It establishes an industry-standard set of biometric identity management services. This will allow applications and systems to be built upon an open-system standard rather than implementing custom one-off solutions for each service provider.
- Eases the implementation of and access to such services since the basic services are pre-defined and can be re-used.
- Facilitates federated, cross-organizational use of biometric services.

1 Scope

BIAS defines biometric services used for identity assurance and invoked over a services-based framework. It is intended to provide a generic set of biometric (and related) functions and associated data definitions to allow remote access to biometric services.

The binding of these services to specific frameworks is not included in this project, but will be the subject of separate standards. The first such standard (for a Web services framework) is planned to be developed by OASIS.

Although focused on biometrics, it will necessarily include support for other related identity assurance mechanisms such as biographic and token capabilities. BIAS is intended to be compatible with and used in conjunction with other biometric standards as described in clause 3.

Specification of single-platform biometric functionality (e.g., client-side capture, etc.) is not within the scope of this standard.

Integration of biometric services as part of an authentication service or protocol (such as WSS) is not within the scope of this standard; however, it is possible that some of the basic biometric services defined herein may be used by such an implementation in the future.

2 Conformance

Annex A specifies the conformance requirements for systems/components claiming conformance to this standard.

3 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.

- OASIS XXX, BIAS Integration Services (Title TBD).
- ISO/IEC 19785-1, Information Technology – Common Biometric Exchange Formats Framework – Part 1: Data Element Specification.
- ISO/IEC 19785-2, Information Technology – Common Biometric Exchange Formats Framework – Part 2: Procedures for the Operation of the Biometric Registration Authority.

4 Terms and Definitions

TBD

5 Symbols and Abbreviated Terms

AFIS – Automated Fingerprint Identification System

API – Application Programming Interface

BIAS – Biometric Identity Assurance Services

BIR – Biometric Information Record

CBEFF – Common Biometric Exchange Formats Framework

ESB – Enterprise Service Bus

GUI – Graphical User Interface

ID – Identity/Identification/Identifier

SOA – Service Oriented Architecture

6 System Context

6.1 Service Oriented Architectures

Service Oriented Architectures (SOA) are software architectures in which reusable services are deployed onto application servers and then consumed by clients in different applications or business processes. They are intended to decouple the implementation of a software service from the interface that calls that service. This allows clients of a service to rely on a consistent interface regardless of the implementation technology of the service [JDJ].

Biometric services are one of the types of services that can be provided over such a remote interface in a distributed information system across a collection of networks. This can occur in a 2-tier, 3-tier, or N-tier environment. A diagram of a simple N-tier architecture is shown in Figure 6-1, below [Alonso].

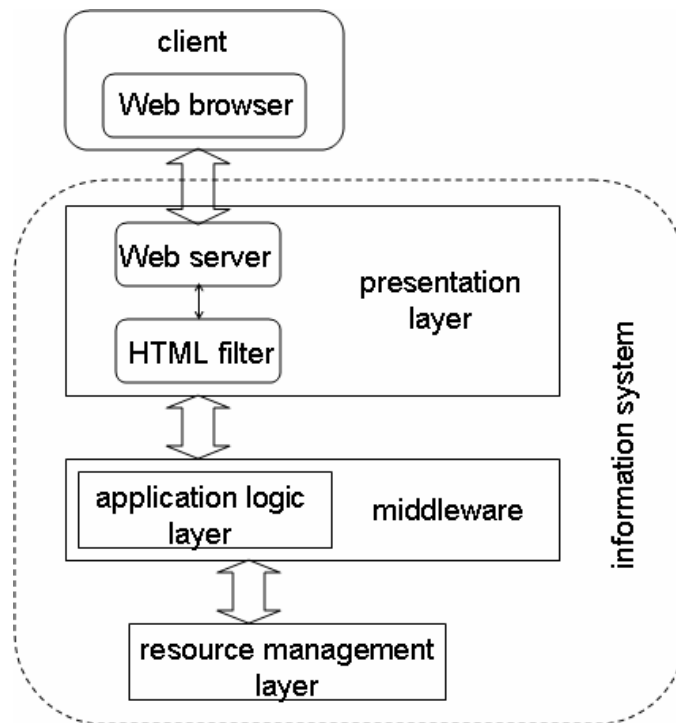


Figure 6-1. Simple N-tier Architecture

In this simple diagram, BIAS services are defined between the application logic layer and the resource management layer.

The biometric resources that are of interest may include one or more of the following (examples):

- A 1:1 fingerprint verification matching server
- A 1:N iris search/match engine
- A facial biometric watch list
- A criminal or civil AFIS system
- A name-based biographic identity database
- An archive of biometric identifiers
- A population of subjects

It is desired that a generic set of services be defined that allows clients to remotely access and manage these capabilities. To the extent possible, domain specific implementations are to be avoided.

NOTE: This standard is intended to support a wide variety of application domains which may include government (e.g., background checking, border management, and criminal justice), enterprise (e.g., logical access control), and commercial biometric identity management implementations (e.g., employee databases).

Services are well defined, self-contained modules that provide standard business functionality and are independent of the state or context of other services and that can be easily assembled to form a collection of autonomous and loosely-coupled business processes. [Papazoglou]

It is not the intention that specific business logic be instantiated within the service definitions – this logic is more appropriate within the application logic layer – either in the higher level system initiating the series of requests, or within the middleware (e.g., an ESB, workflow manager, or biometric middleware) as appropriate. To do so would of necessity make the interface less generic, modular, and flexible and require that the interface be updated each time the logic changed, defeating one of the primary purposes of the services architecture.

The services to be defined are not targeted at a particular SOA implementation or framework. Instead, they are defined in such a manner as to be able to be utilized within any such architecture. This is accomplished by separately defining (in another standard) the bindings to that architecture/implementation. For example, Web services bindings are defined in OASIS xxx, BIAS Integration Services (referenced TBD).

6.2 BIAS Architecture

The BIAS architecture consists of the following components:

- BIAS services (interface definition)
- BIAS data (schema definition)
- BIAS bindings (defined outside this standard)

The BIAS services interface exposes a common set of operations to external requesters of these operations. These requesters may be an external system, a web application, or an intermediary. The BIAS services themselves are platform and language independent.

BIAS services provide basic biometric functionality as modular and independent operations which can be assembled in many different ways to perform a variety of business processes.

Figure 6-2 depicts the BIAS services within an application environment.

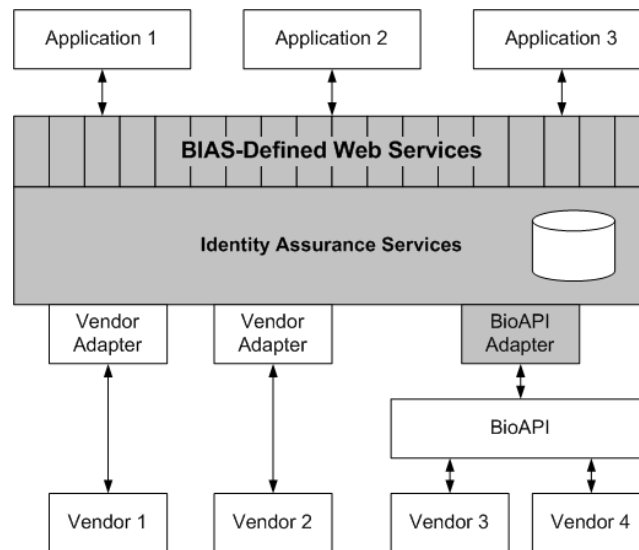


Figure 6-2. BIAS Application Environment

In defining BIAS services, it may be useful to define a set of primitive operations (baseline) as well as a set of higher level ‘combination’ functions which group primitive operations into a single request for those that are commonly associated.

6.3 BIAS Requirements

Biometric services, and the applications which use them, particularly in an identity assurance context, imply some unique requirements which are summarized below:

- Some services can be performed very quickly while others (such as a 1:N identification within a large population) can take considerable time (on the order of hours) to complete. Therefore, the interface must support both synchronous and asynchronous operations.
- Upon update of a record within a biometric/identity resource, notification of either the owner/originator of that record or of a 3rd party may be required. Therefore, the ability to setup and execute such notifications (initiated from the service side) is needed.
- Some primitive services lend themselves to natural groupings and sequencing – this may justify creation of some ‘aggregate services’ which perform a series of primitive operations based on a single request. [An example of such a grouping would be a negative search in which a 1:N identification which results in a ‘no match’ is immediately followed by the addition of the sample biometric record into that search population.]
- Biometric operations may be singular or multi-biometric.
- Some systems are “person-centric” and others are “encounter-centric”. That is, some base transactions on a unique identifier associated with an individual

human being while others track “biometric encounters” which may or may not be linked through such an identifier.

- Biometric data is in nearly all cases considered personal information and thus privacy protection is always a consideration.

7 Biometric Services

7.1 Primitive Services

BIAS offers the following set of primitive services.

7.1.1 Add Subject to Gallery

The Add Subject to Gallery service registers a subject to a given gallery or population group. As an optional parameter, the value of the claim to identity by which the subject is known to the gallery may be specified. This claim to identity must be unique. If no claim to identity is specified, the subject ID (assigned with the Create Subject service) will be used as the claim to identity. Additionally, in the encounter-centric model, the encounter ID associated with the subject’s biometrics that will be added to the gallery must be specified.

Parameters:

- Input
 - Gallery ID
 - Subject ID
 - Identity Claim
 - (conditional) Encounter ID
- Output
 - None

7.1.2 Check Background

TBD – BIAS recognizes the need to provide a capability to search other systems. The format and even the name of this service are still being discussed.

7.1.3 Check Quality

The Check Quality service returns a quality score for a given biometric.

Parameters:

- Input

- Biometric Data
- Output
 - Quality Score
 - Quality Algorithm Vendor
 - Quality Algorithm
 - Quality Algorithm Version

NOTE: It may be possible to create a single “Algorithm ID”, consisting of an ‘Algorithm Owner’ and ‘Algorithm Type’ which can be assigned in the same manner as a Format ID or Product ID. (For discussion.)

7.1.4 *Classify Biometric Data*

TBD

7.1.5 *Create Subject*

The Create Subject service creates a new subject record and associates a subject ID to that record. The subject ID may be specified by the caller in an optional parameter or generated by the service.

Parameters:

- Input
 - (optional) Subject ID
- Output
 - Subject ID

7.1.6 *Delete Biographic Data*

The Delete Biographic Data service removes biographic data from a given subject record. In the encounter-centric model, the encounter ID must be specified.

Parameters:

- Input
 - Subject ID
 - (conditional) Encounter ID
- Output
 - None

7.1.7 Delete Biometric Data

The Delete Biometric Data service removes biometric data from a given subject record. In the encounter-centric model, the encounter ID must be specified.

Parameters:

- Input
 - Subject ID
 - (conditional) Encounter ID
- Output
 - None

7.1.8 Delete Subject

The Delete Subject service deletes an existing subject record and, in an encounter-centric model, any associated encounter information from the system. This service will also remove the subject from any registered galleries.

Parameters:

- Input
 - (optional) Subject ID
- Output
 - Subject ID

7.1.9 Delete Subject from Gallery

The Delete Subject from Gallery service removes the registration of a subject from a gallery or population group. The subject may be identified by either the subject ID or the claim to identity that was specified in the Add Subject to Gallery service.

Parameters:

- Input
 - Gallery ID
 - Subject ID or Identity Claim
- Output
 - None

7.1.10 Identify Subject

The Identify Subject service performs an identification search against a given gallery for a given biometric, returning a rank-ordered candidate list of a given maximum size.

Parameters:

- Input
 - Gallery ID
 - Biometric Data
 - Max List Size
- Output
 - Candidate List

NOTE: Search parameters and controls, and how they are specified, need to be considered.

7.1.11 List Biographic Data

The List Biographic Data service lists the biographic data elements stored for a subject. In the encounter-centric model, an encounter ID may be specified to indicate that only the biographic data elements stored for that encounter should be returned. If an encounter ID is not specified and encounter data exists for the subject, the service will return the list of encounter IDs which contain biographic data.

Parameters:

- Input
 - Subject ID
 - (optional) Encounter ID
- Output
 - List of Biographic Data Elements or List of Encounter IDs

7.1.12 List Biometric Data

The List Biometric Data service lists the biometric data elements stored for a subject. In the encounter-centric model, an encounter ID may be specified to indicate that only the biometric data elements stored for that encounter should be returned. If an encounter ID is not specified and encounter data exists for the subject, the service will return the list of encounter IDs which contain biometric data.

An optional parameter may be used to indicate a filter on the list of returned data. Such a filter may indicate that only biometric types should be listed (e.g. face, finger, iris, etc...), that all biometric information should be listed (e.g. left index finger, right iris, face frontal, etc...), or that only biometric information for a particular biometric type should be listed (e.g. all fingerprints: left slap, right index, etc...).

Parameters:

- Input
 - Subject ID
 - (optional) Encounter ID
 - (optional) List Filter
- Output
 - List of Biographic Data Elements or List of Encounter IDs

7.1.13 Perform Fusion

TBD

7.1.14 Retrieve Biographic Information

The Retrieve Biographic Information service retrieves the biographic data associated with a subject ID. In the encounter-centric model, either the encounter ID may be specified or the service will return the information associated with the most recent encounter.

Parameters:

- Input
 - Subject ID
 - (optional) Encounter ID
- Output
 - Biographic Data

7.1.15 Retrieve Biometric Information

The Retrieve Biometric Information service retrieves the biometric data associated with a subject ID. In the encounter-centric model, either the encounter ID may be specified or the service will return the information associated with the most recent encounter.

Parameters:

- Input
 - Subject ID
 - (optional) Encounter ID
- Output
 - Biometric Data

7.1.16 Set Biographic Data

The Set Biographic Data service associates biographic data for a given subject record. An input flag indicates whether the biographic information should replace any existing biographic information (person-centric model) or if a new encounter should be created and associated with the subject (encounter-centric model). For encounter-centric models, the encounter ID may be specified by the caller in order to link biographic and biometric information (assuming biometric information was previously associated using the Set Biometric Data service). If the encounter ID is omitted for the encounter-centric model, the service will return a system-assigned encounter ID.

Parameters:

- Input
 - Subject ID
 - Identity Model
 - (optional) Encounter ID
 - Biographic Details
- Output
 - (if Identity Model = encounter-centric) Encounter ID

7.1.17 Set Biometric Data

The Set Biometric Data service associates biometric data for a given subject record. An input flag indicates whether the biometric information should replace any existing biometric information (person-centric model) or if a new encounter should be created and associated with the subject (encounter-centric model). For encounter-centric models, the encounter ID may be specified by the caller in order to link biographic and biometric information (assuming biographic information was previously associated using the Set Biographic Data service). If the encounter ID is omitted for the encounter-centric model, the service will return a system-assigned encounter ID.

Parameters:

- Input
 - Subject ID
 - Identity Model
 - (optional) Encounter ID
 - Biometric Details
- Output
 - (if Identity Model = encounter-centric) Encounter ID

7.1.18 Transform Biometric Data

The Transform Biometric Data service transforms or processes a given biometric in one format into a new target format. Examples of transformations include:

- Feature Extraction
- Centering or cropping biometric images
- Standard biometric data format conversion
- Etc...

Parameters:

- Input
 - Biometric Data
 - Transform Operation
- Output
 - Biometric Data in new format

7.1.19 Update Biographic Data

The Update Biographic Data service updates the biographic data for an existing subject record. In the encounter-centric model, the encounter ID must be specified.

Parameters:

- Input
 - Subject ID
 - (conditional) Encounter ID
- Output

- None

7.1.20 Update Biometric Data

The Update Biometric Data service updates the biometric data for an existing subject record. In the encounter-centric model, the encounter ID must be specified. In the person-centric model, an input flag indicates if the input biometric data should either replace or be merged with the existing biometric data.

Parameters:

- Input
 - Subject ID
 - (conditional) Encounter ID
 - (optional) Merge
- Output
 - None

7.1.21 Verify Subject

The Verify Subject service performs a 1:1 verification match between a given biometric and either a claim to identity in a given gallery or another given biometric.

Parameters:

- Input
 - Sample Biometric
 - (optional) Gallery ID
 - (optional) Identity Claim
 - (optional) Reference Biometric
- Output
 - Match Decision
 - Match Score

NOTE: Search parameters and controls, and how they are specified, need to be considered.

7.2 Aggregate Services

BIAS offers the following set of aggregate services. The intent of BIAS is to standardize the service request; system requirements and organizational business rules will determine how the service is implemented.

7.2.1 *Enroll*

The Enroll aggregate service adds a new subject or, in an encounter-centric model, a new encounter to the system. This may be accomplished in a number of different ways according to system requirements and/or resources. For example, this aggregate service may initiate one or more Identify Subject service requests to determine if the given subject is already known to the system. If the subject is not previously known to the system, any or all of the Create Subject, Set Biographic Data, Set Biometric Data, and Add Subject to Gallery services may be utilized to add subject information to the system. If the subject is previously known to the system, the service may (1) do nothing; (2) initiate an Update Biographic Data and/or Update Biometric Data service request in a person-centric model; or (3) initiate a Set Biographic Data and/or Set Biometric Data service request in an encounter-centric model.

Parameters:

- Input
 - Biometric Data
 - Biographic Data
 - (optional) Processing Options
- Output
 - (conditional) Subject ID
 - (conditional) Encounter ID

7.2.2 *Identify*

The Identify aggregate service performs an identification function according to system requirements and/or resources. For example, a system may have multiple galleries of subjects, and may utilize any or all of these galleries, via calls to the Identify Subject service, to perform a system-level identification function. The system may perform additional actions based on input flags and/or results of the Identify Subject service requests. For example, in an encounter-centric model, this aggregate service may search three separate galleries of subjects, and if a match is found it may then utilize the Set Biographic Data and/or Set Biometric Data services to create a new encounter for the subject.

Parameters:

- Input
 - Biometric Data
 - (optional) Biographic Data
 - (optional) Processing Options

- Output
 - (conditional) Subject ID (s)
 - (conditional) Encounter ID (s)

7.2.3 Retrieve Information

The Retrieve Information aggregate service retrieves requested information about a subject, or in an encounter-centric model about an encounter. In a person-centric model, this aggregate service may be used to retrieve both biographic and biometric information for a subject record. In an encounter-centric model, this aggregate service may be used to retrieve biographic and/or biometric information for either a single encounter or all encounters.

Parameters:

- Input
 - Subject ID or Encounter ID
 - (optional) Information Filter
- Output
 - (conditional) Biographic Data
 - (conditional) Biometric Data

7.2.4 Verify

The Verify aggregate service performs a 1:1 verification function according to system requirements and/or resources. The system may perform additional actions based on input flags and/or results of verification. For example, in an encounter-centric model, this aggregate service may initiate a request to the Verify Subject service, and if a match is found it may then utilize the Set Biographic Data and/or Set Biometric Data services to create a new encounter for the subject.

Parameters:

- Input
 - Biometric Data
 - Identity Claim
 - (optional) Biographic Data
 - (optional) Processing Options
- Output
 - Match Decision

- (conditional) Subject ID
- (conditional) Encounter ID

8 Data Elements

TBD: A goal of BIAS is to be flexible to the amount and types of biographic and biometric information available to and used by a system. The parameters “Biographic Data” and “Biometric Data” are meant to be general in this sense in order to allow this flexibility. This section is intended to include information on how this flexibility can be specified and supported by implementing systems.

NOTE: A generic set of data elements needs to be discussed, agreed to, and defined. The services in Clause 7 imply the following data elements/groups:

- Biographic Data
- Biometric Data
- Candidate List
- Encounter ID
- Gallery ID
- Identity Claim
- Match Decision
- Match Score
- Reference Biometric
- Quality Algorithm
- Quality Algorithm Vendor
- Quality Algorithm Version
- Quality Score
- Sample Biometric
- Subject ID

9 Error Handling and Notification

Based upon the nature of a web service environment there is a need to define effective measures for error handling and system notifications.

The Session Initiation Protocol (SIP) is a very applicable solution for handling this need for many reasons. At the root of its applicability is the advantage that SIP is a simple protocol that is easily integrated with other common established protocols, mainly the Internetworking Protocol (IP). As it relates to this web service environment, SIP also integrates rather easily with HTTP and other web-based protocols.

“In large part because SIP borrows heavily from HTTP and other internet standards from the IETF, lots of web-like technologies can be used to build SIP

applications. SIP development looks and feels a lot like web development, and there are a lot of web developers out there.”¹

The robust notification functionality of SIP stems from the ability to produce messages in a wide range of multimedia forms. These methods are already very much common place in industry and government such as email and text messaging. The recent emergence of mobile technologies can provide tremendous avenues in which SIP can be utilized to distribute notifications in addressing the needs of varying systems.

10 Security

Security is important for any kind of distributed computing environment, and even more so when distributed computing occurs over open networks. Web services generally operate as a public internet web service, an intranet web service, or a combination of both. The following security concerns need to be addressed in an SOA:

- Message confidentiality and integrity.
- Transport confidentiality and integrity.
- Preventing exceptions from revealing information about the service architecture.
- Protecting the service from spurious messages.

Currently, SSL (Secure Socket Layer) is the most common security scheme used by web services, along with several XML based security initiatives also being pursued. The OASIS Web Services Security (WSS) Technical Committee is working on web services security for higher level security services. The scope of this Technical Committee includes support of security mechanisms that use XML digital signatures and XML encryption to provide SOAP message confidentiality and integrity, and carrying security information for multiple parties². The OASIS Web Services Secure Exchange (WS-SX) Technical Committee is defining extensions to the OASIS WSS to enable trusted SOAP message exchanges involving multiple message exchanges. The OASIS WSS specification describes a base mechanism for securing SOAP messages but does not deal with trust brokering, multi-message exchanges, and policies describing how to secure message exchanges with a web service³.

The OASIS Security Services Technical Committee (SSTC) is involved in defining, enhancing, and maintaining a standard XML-based framework for creating and exchanging authentication and authorization information. Currently

¹ <http://www.sipcenter.com/sip.nsf/html/IMS+IP+Multimedia+Subsystem>

² More information can be found at <http://www.oasis-open.org/committees/wss/charter.php>

³ More information can be found at <http://www.oasis-open.org/committees/ws-sx/charter.php>

Security Assertions Markup Language (SAML) is at Version 2.0, which is used by architectures that require interoperable security solutions⁴.

⁴ More information can be found at <http://www.oasis-open.org/committees/security/charter.php>

Annex A Conformance Requirements

TBD

Annex B Bibliography

- ISO/IEC FDIS 19784.1 BioAPI Specification – Part 1
- ISO/IEC 2ndWD 19784.1 BioAPI Specification – Part 2, Biometric Archive Function Provider Interface
- ISO/IEC WD 24708, BioAPI Interworking Protocol (BIP)
- <http://msdn.microsoft.com/webservices/default.aspx?pull=/library/en-us/dnpag2/html/wssp.asp>
- <http://www.sipcenter.com/sip.nsf/html/IMS+IP+Multimedia+Subsystem>
- [JDJ] Service-Oriented Architecture: Beyond Web Services, JDJ, http://java.sys-con.com/read/44368_p.htm
- [Alonso] *Web Services – Concepts, Architectures, and Applications*, Alonso, Casati, Kuno and Machiranjju, Springer, 2004

Annex C Example Usage Scenarios

TBD

Annex D: Issues to be Resolved (Temporary Annex)

The following list of issues have been identified and still need to be discussed and resolved:

- 1) Definition of data elements and the underlying data model
- 2) The ability to monitor services that need to comply with established service level agreements
- 3) Identification and Verification search parameters (e.g. thresholds)
- 4) Asynchronous and synchronous operations
- 5) System notification processing
- 6) The “Check Background” service and integrating with other identity assurance systems
- 7) Determination and/or specification of the “Processing Options” parameter for several of the aggregate services; should they be defined in the standard or by the system implementation?
- 8) Define and detail the remaining primitive services (marked as TBD).
- 9) Provide a context diagram and explanation around concepts of Subjects, Encounters, and Galleries.
- 10) Mechanism for discovering capabilities, supported options, gallery information, etc...