

M1/05-0830

Title: BIAS specification outline

Source: Project sponsors (Daon, SAFLINK, DHS)

Date: 30 November 2005

Comments: For discussion at 14/15 Dec meeting of M1.2

References: M1/05-0788, M1/05-0789

InterNational Committee for Information Technology Standards
INCITS Secretariat, Information Technology Industry Council (ITI)
1250 Eye St. NW, Room 200, Washington, DC 20005
Telephone 202-737-8888; Fax 202-638-4922
email: incits@itic.org

Biometric Identity Assurance Services (BIAS)

Project INCITS xxxx

Proposed Outline

Revision History

Revision	Date	M1 Document	Comment
0.1	30 Nov 2005	M1/05-0830	Proposed Outline

Table of Contents

1. Scope.....	6
2. Conformance.....	7
3. Normative References.....	7
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.....	8
7. Biometric Services.....	8
8. Data Elements.....	10
9. Error Handling.....	10
10. Security.....	10
Annex A. Conformance Requirements.....	10
Annex B. Bibliography.....	10
Annex C. Example Usage Scenarios.....	11

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. BIAS 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 (but 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 US-VISIT (and other DHS programs) to build 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 cross-agency use of biometric services.

1. Scope

The Biometric Identity Assurance Services (BIAS) specification 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.

2. Conformance

3. Normative References

4. Terms and Definitions

5. Symbols and Abbreviated Terms

6. System Context

Describe the context for BIAS. Include architecture information and diagrams to help illustrate.

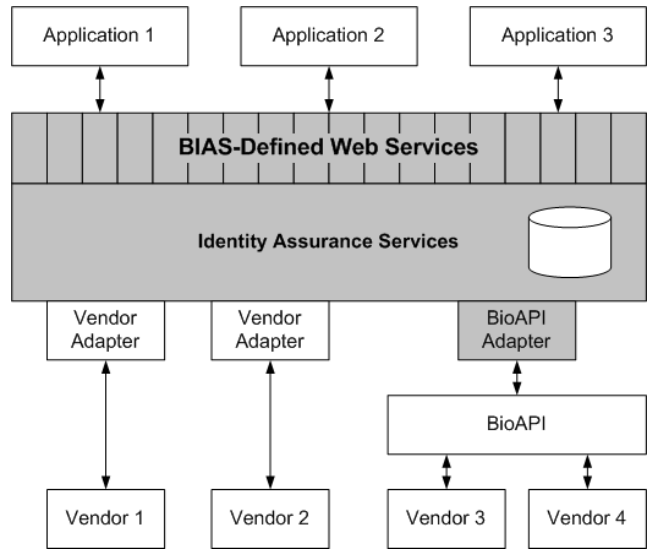
6.1. Service Oriented Architectures

Describe how/where BIAS fits in.

Talk about what level of services are required.

Discuss where business logic is applied.

Talk about bindings to various services-frameworks.



6.2. BIAS Architecture

7. Biometric Services

Each service will have it's own 7.x heading to define the service (inputs, process, and outputs).

Below is a draft set of biometric services to be defined.

Function	Description	Relationship to BioAPI
AddSubjectToPopulation	Registers a subject to a given population. Include an optional parameter to specify the value of the claim to identity. If this parameter is omitted, the subjectID (assigned with the CreateSubject function) will be used as the claim to identity.	
CheckBackground	Placeholder - potential inclusion of external law enforcement functions/integration	
CheckQuality	Returns a quality score on biometric data - details TBD	
ClassifyBiometricData	Classifies biometric data - details TBD	
CreateSubject	Create a new subject record. Include an optional parameter to specify the subject ID. If this parameter is omitted, the system will generate one. Return the assigned subject ID.	
DeleteBiographicData	Deletes biographic data from a subject record. If version numbers are tracked, then the version number needs to be specified as a parameter.	
DeleteBiometricData	Deletes biometric data from a subject record. If version numbers are tracked, then the version number needs to be specified as a parameter.	BioAPI_DbDeleteBIR

DeleteSubject	Deletes the subject record from the system including any populations it is registered to.	
DeleteSubjectFromPopulation	Removes the registration of a subject from a given population.	
EnumerateBiographicData	Enumerates the list of biographic data elements stored for a subject. If version numbers are tracked, then the version number needs to be specified as a parameter or information on the last (highest) version of data will be returned.	
EnumerateBiometricData	Enumerates the biometric data types stored for a subject. If version numbers are tracked, then the version number needs to be specified as a parameter or information on the last (highest) version of data will be returned.	
GetBiographicData	Retrieve data elements from subject record (e.g. SSN). If version numbers are tracked, then the version number needs to be specified as a parameter or the last (highest) version of data will be returned.	
GetBiometricData	Retrieve biometric data from subject record. If version numbers are tracked, then the version number needs to be specified as a parameter or the last (highest) version of data will be returned.	BioAPI_DbGetBIR, BioAPI_DbGetNextBIR
IdentifySubject	Identification function against a population returning a rank ordered candidate list with the maximum list size specified by an integer parameter.	BioAPI_Identify, BioAPI_IdentifyMatch
Perform fusion	Future - pending ongoing research and standards development. As a minimum, must address score level fusion.	
SetBiographicData	Set biographic data elements for a subject record (e.g. SSN). Include a parameter that specifies if a new version should be created to allow multiple instances of the same biographic information. Include an optional parameter to specify the version number in order to link biographic and biometric information. If a new version is requested and the version number is omitted, the function will return a system-assigned version number. If a new version is requested and a version number is supplied, but the version number already exists, the function will return an error.	
SetBiometricData	Set biometric data for a subject record. Include a parameter that specifies if a new version should be created to allow multiple instances of the same biometric. Include an optional parameter to specify the version number in order to link biographic and biometric information. If a new version is requested and the version number is omitted, the function will return a system-assigned version number. If a new version is requested and a version number is supplied, but the version number already exists, the function will return an error.	BioAPI_StoreBIR
TransformBiometricData	Transform biometric data into a target format - for example, feature extraction, format translation etc.	BioAPI_Process, BioAPI_CreateTemplate (also BioAPI_Import)
UpdateBiographicData	Update biographic data. If version numbers are tracked, then the version number needs to be specified.	

UpdateBiometricData	Update biometric data. If version numbers are tracked, then the version number needs to be specified. Include a flag to allow adaptation (merge) with existing data.	Update: BioAPI_Enroll Adaptation: BioAPI_Verify (and VerifyMatch).
VerifySubject	Perform a 1:1 match against a specified population for a submitted biometric sample and claim of identity. Function should support matching to an enrolment sample provided in a database or provided by the service call directly.	BioAPI_Verify, BioAPI_VerifyMat ch

Notes

No user interface with this standard

8. Data Elements

Describe the data format flexibility for service parameters and how that format is controlled/defined.

9. Error Handling

Describe how errors are handled and communicated.

10. Security

Describe how security is handled in the services.

Annex A. Conformance Requirements

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 FDIS 19785.1, Common Biometric Exchange File Formats Framework: Part1: Data Element Specification
- ISO/IEC FDIS 19785.2, Common Biometric Exchange File Formats Framework: Part2: Procedures for the Operation of the Biometrics Registration Authority
- ISO/IEC WD 24708, BioAPI Interworking Protocol (BIP)

Annex C. Example Usage Scenarios