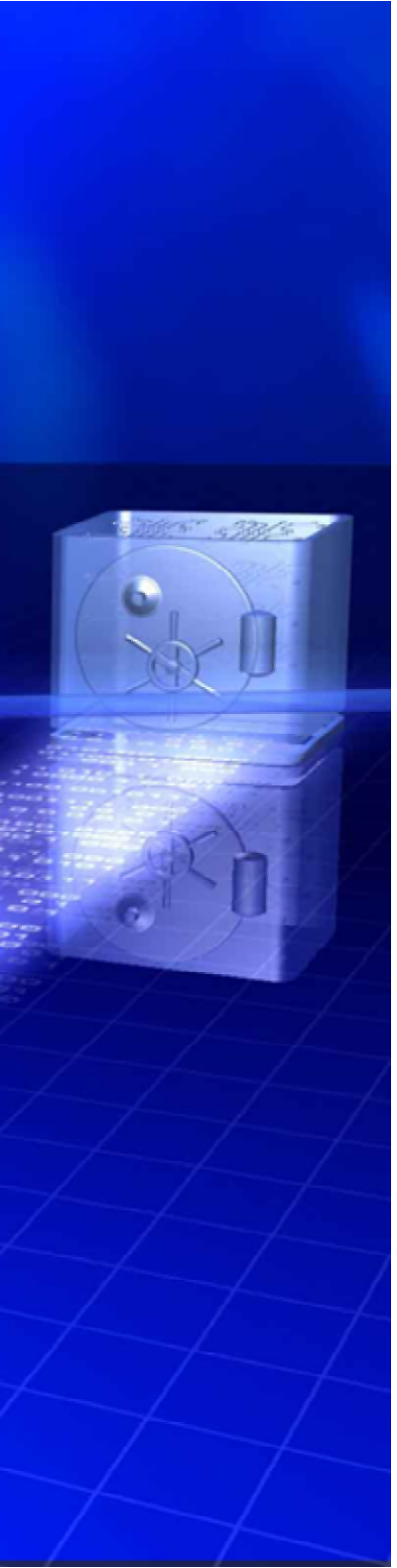
Biometric Standards – Overview and Status

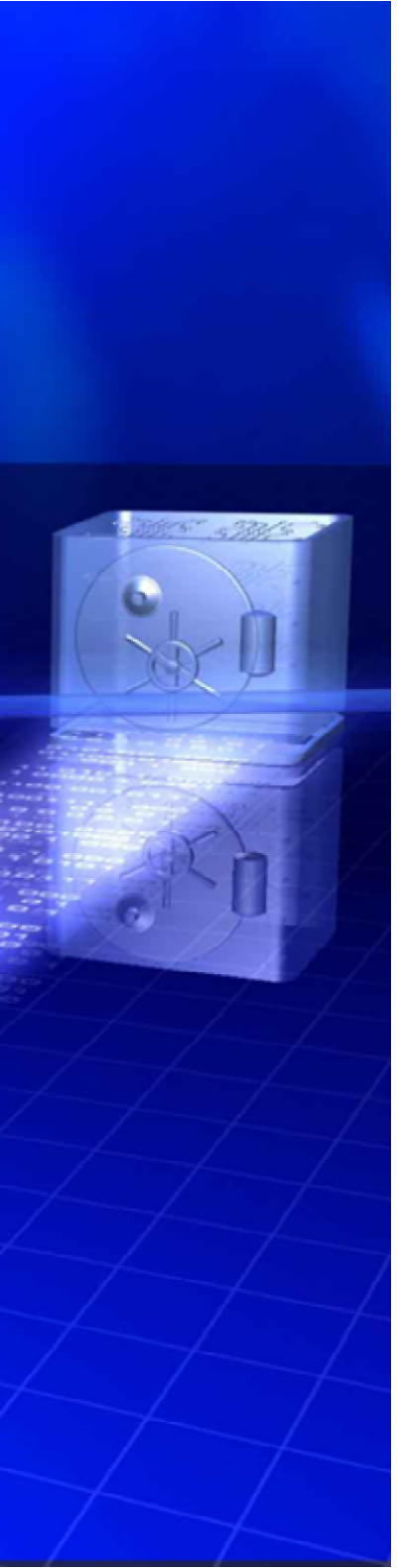
SAFLINK Corporation

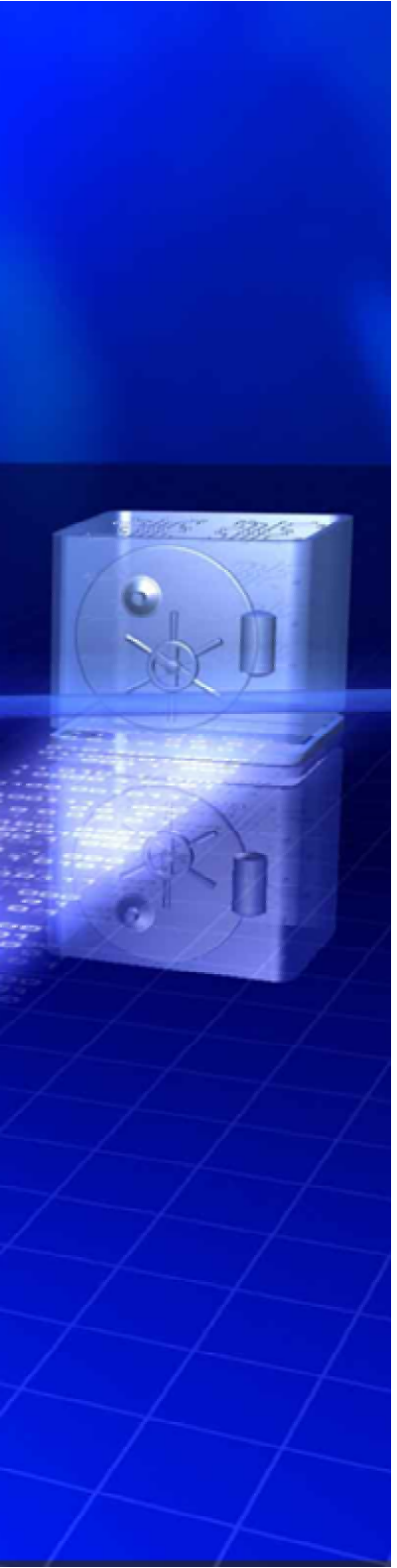


Standards Scene

- INCITS – International Committee on Information Technology Standards
  - B10: Cards & Personal ID
  - M1: Biometrics
- ISO – International Organization for Standardization
  - JTC1/SC17: Cards & Personal ID
  - JTC1/SC37: Biometrics
  - JTC1/SC27: IT Security
  - TC68: Financial Services
- Informal Bodies
  - BioAPI Consortium
  - JCF

What's going on?





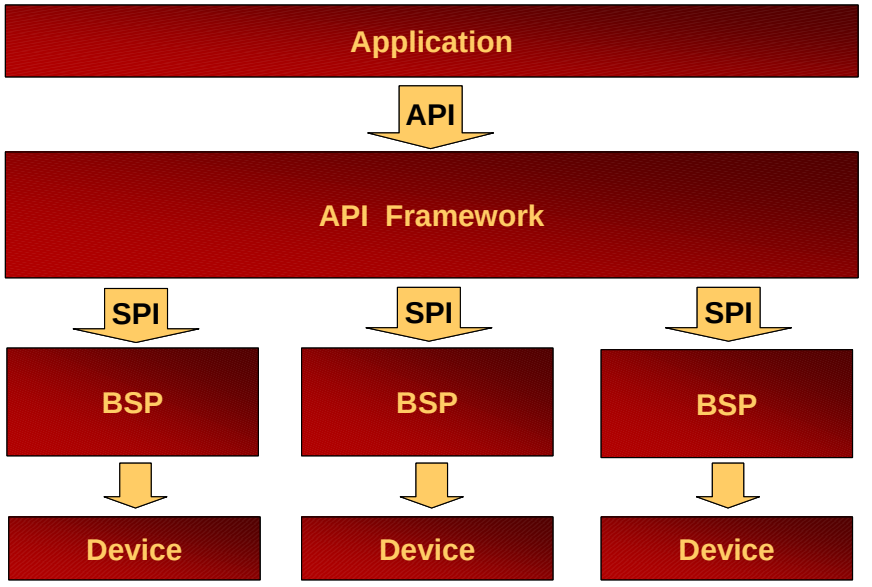
SC37 Structure

SG1	Harmonized Biometric Vocabulary and Definitions	Canada
SG2	Biometric Technical Interfaces	Korea
SG3	Biometric Data Interchange Formats	Germany
SG4	Profiles for Biometric Applications	USA
SG5	Biometric Testing and Reporting	UK
SG6	Cross Jurisdictional and Societal Aspects	Italy

BioAPI

ANSI/INCITS 358

- The BioAPI Specification defines an open system standard application program interface (API) that allows software applications to communicate with a broad range of biometric technologies in a common way.



- ✓ Simple application interfaces,
- ✓ Standard access methods to biometric functions, algorithms, and devices,
- ✓ Robust biometric data management and storage,
- ✓ Standard methods of managing biometric data and technology types, and
- ✓ Support for biometric verification and identification in distributed computing environments.

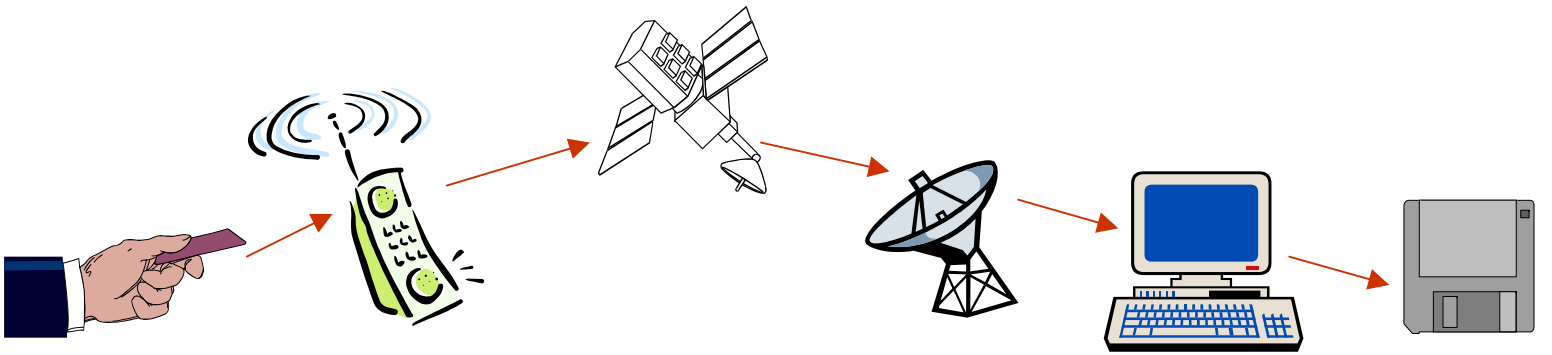
ANSI

incits InterNational Committee for Information Technology Standards
here IT all begins

CBEFF
Common Biometric Exchange File Format

NISTIR 6529
www.nist.gov/cbeff

CBEFF describes a set of data elements necessary to support biometric technologies in a common way.



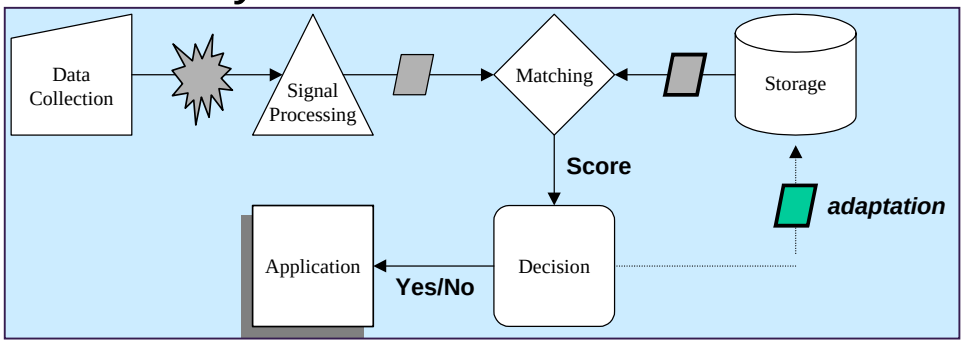
- Spearheaded by NIST and the BC
- Developed in coordination with:
  - The BioAPI Consortium
  - ANSI X9F4 Working Group (Financial Services)
  - The International Biometric Industry Association
  - The Interfaces Group of TeleTrusT (Germany)

- Features:
  - Facilitates biometric data interchange between different system components or systems
  - Promotes interoperability of biometric-based application programs and systems
  - Provides forward compatibility for technology improvements
  - Simplifies the software and hardware integration process

ANSI X9.84

In ballot as ISO TC68 CD 19092

- X9 - Financial Services
  - X9F - Information & Data Security
    - X9F4 - Cryptographic Applications
      - **X9.84 – 2003 Biometric Info. Mgmt. & Security**
- X9.84 Scope
  - Security of biometric data across its life cycle
  - Management of the biometric data across its life cycle
  - Usage of biometric technology for *verification* and *identification* banking customers and employees
  - Application of biometric technology for physical and logical access controls
  - Encapsulation of biometric data
  - Techniques for securely transmitting and storing biometric data
  - Security of the physical hardware used throughout the biometric life cycle



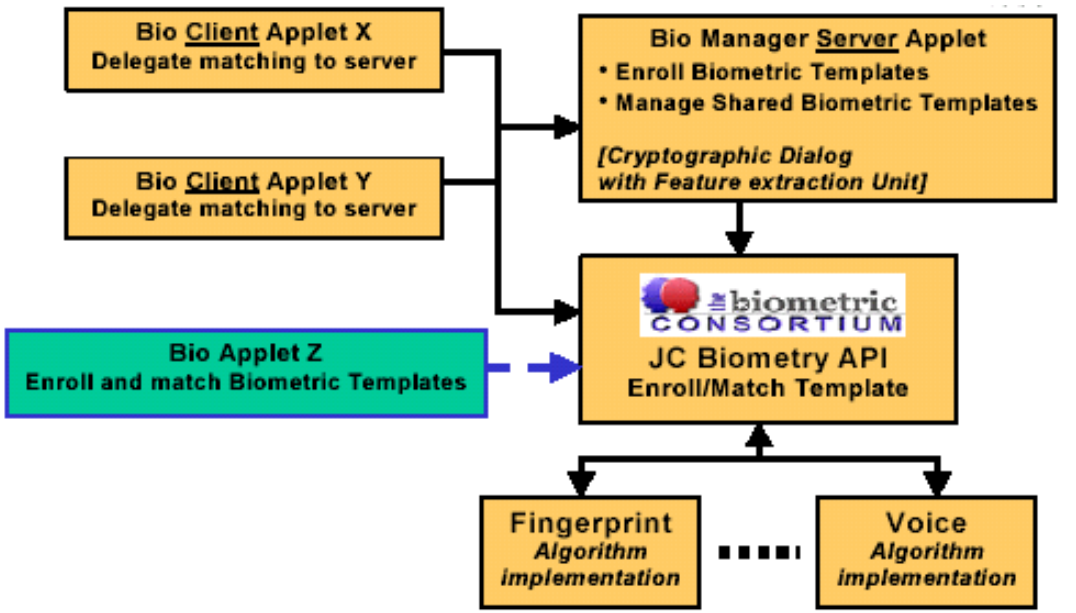
OASIS XCBF

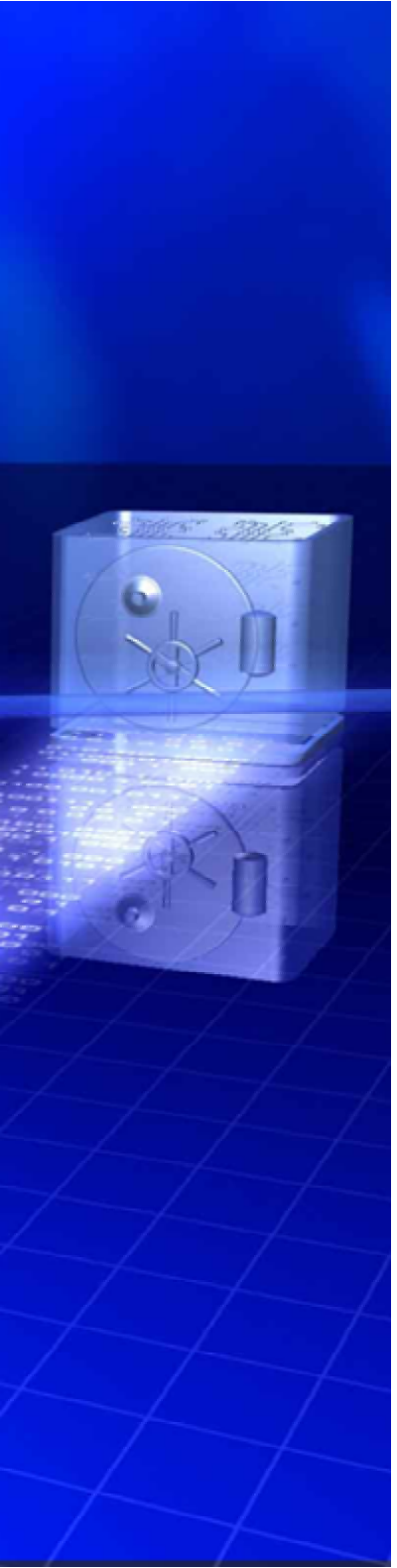
- **Organization for the Advancement of Structured Information Standards (OASIS)**
  - eXtensible Markup Language (XML)
  - XML Common Biometric Format Technical Committee (XCBF) WG
- **What is XCBF*?***
  - A Security Standard that defines a common XML markup for two US binary biometrics standards - X9.84:2003 & BioAPI 1.1
  - Instantiation of CBEFF
  - Simple Signature, MAC, HMAC & Encryption for XML markup relies on the same proven, efficient processing used for binary formats in *IETF SMIME, RSA PKCS #7, SET, X9.73 CMS, …*
- **What does XCBF look like*?***
  - An ASN.1 Schema for XML – markup is encoded in a canonical variant of the ASN.1 XML Encoding Rules (cXER)
  - Common Cryptographic Processing for binary & XML markup
- **What is the current status*?***
  - Ver 1.0 published in Feb 2003
- **For more information:**

  http://www.oasis-open.org/committees/xcbf

JCF Biometric API for JavaCard

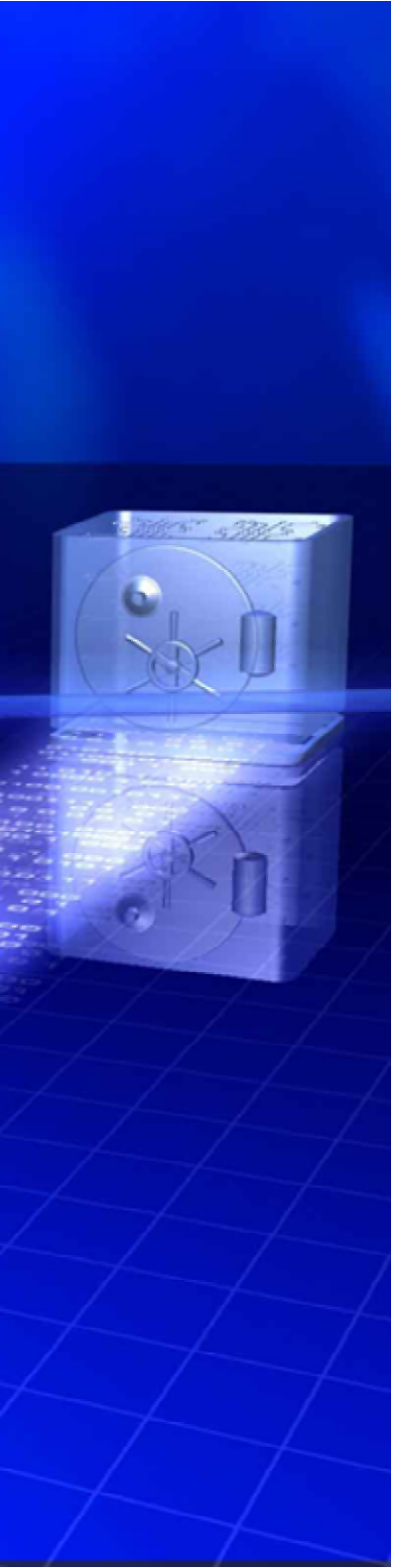
- Goal: Facilitate match-on-card
- Use Javacard for:
  - Securely enrolling/managing biometric templates
    - Templates stored on card
  - Making comparison and granting rights
    - No sensitive information sent off card
- Status:
  - Submitted to M1 as candidate for Fast Track processing





INCITS M1 AHGBISGF

- Ad Hoc Group on Biometric Interoperability in Support of the Government Smart Card Framework
- Chartered August 2002; First meeting January 2003
- Tasking:
  - Study the sufficiency of ANSI/INCITS 358-2002 (BioAPI) and NISTIR 6529-A (CBEFF) to meet the interoperability requirements of NISTIR 6887 (GSC-IS) v2.0 and planned additions through 2.2.
  - Study related standards (7816-11, etc.)
  - Recommend edits/extensions to these standards
- Basically:
  - Figure out how these 2 infrastructures can/should be integrated to support combined use of these synergistic technologies

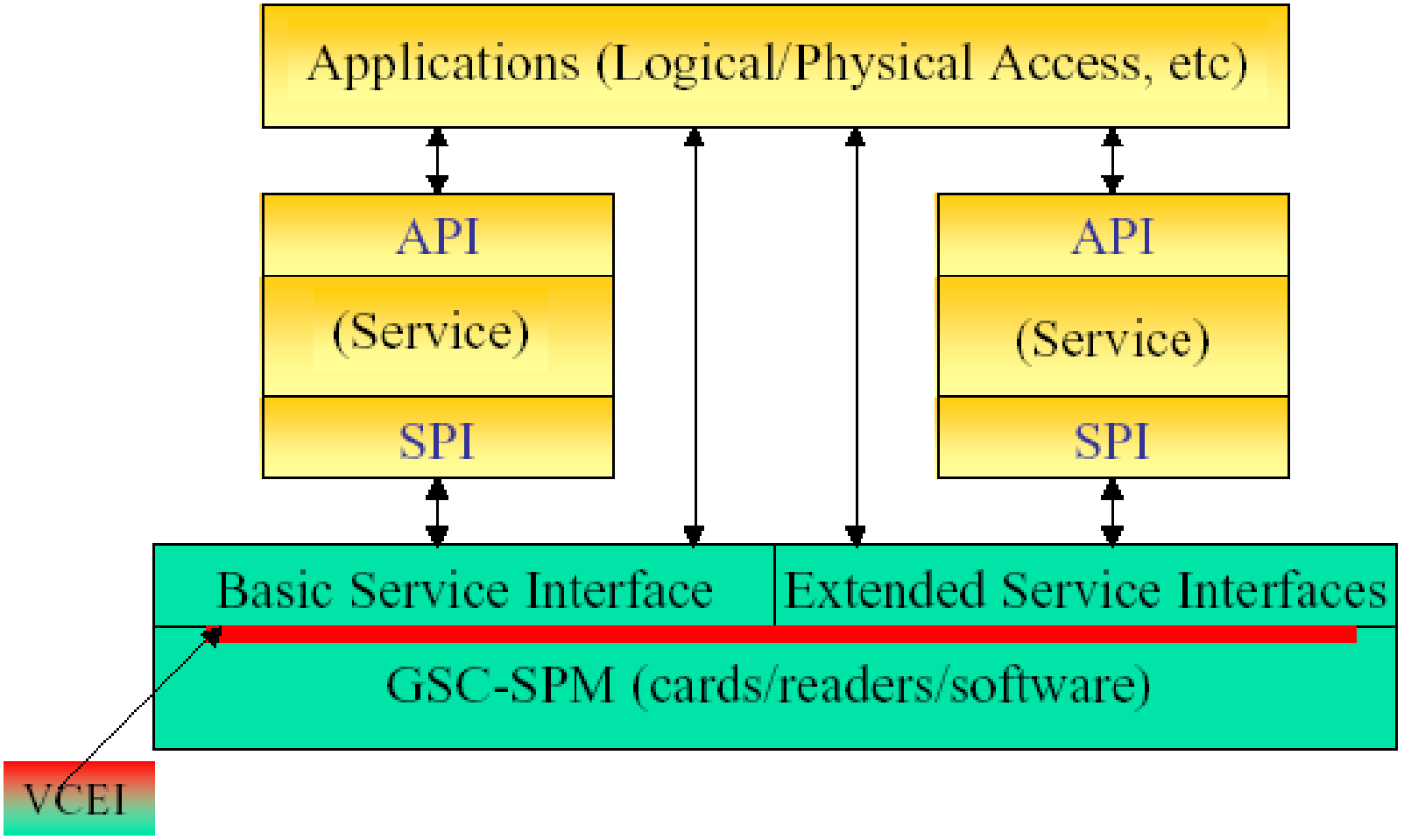


Approach

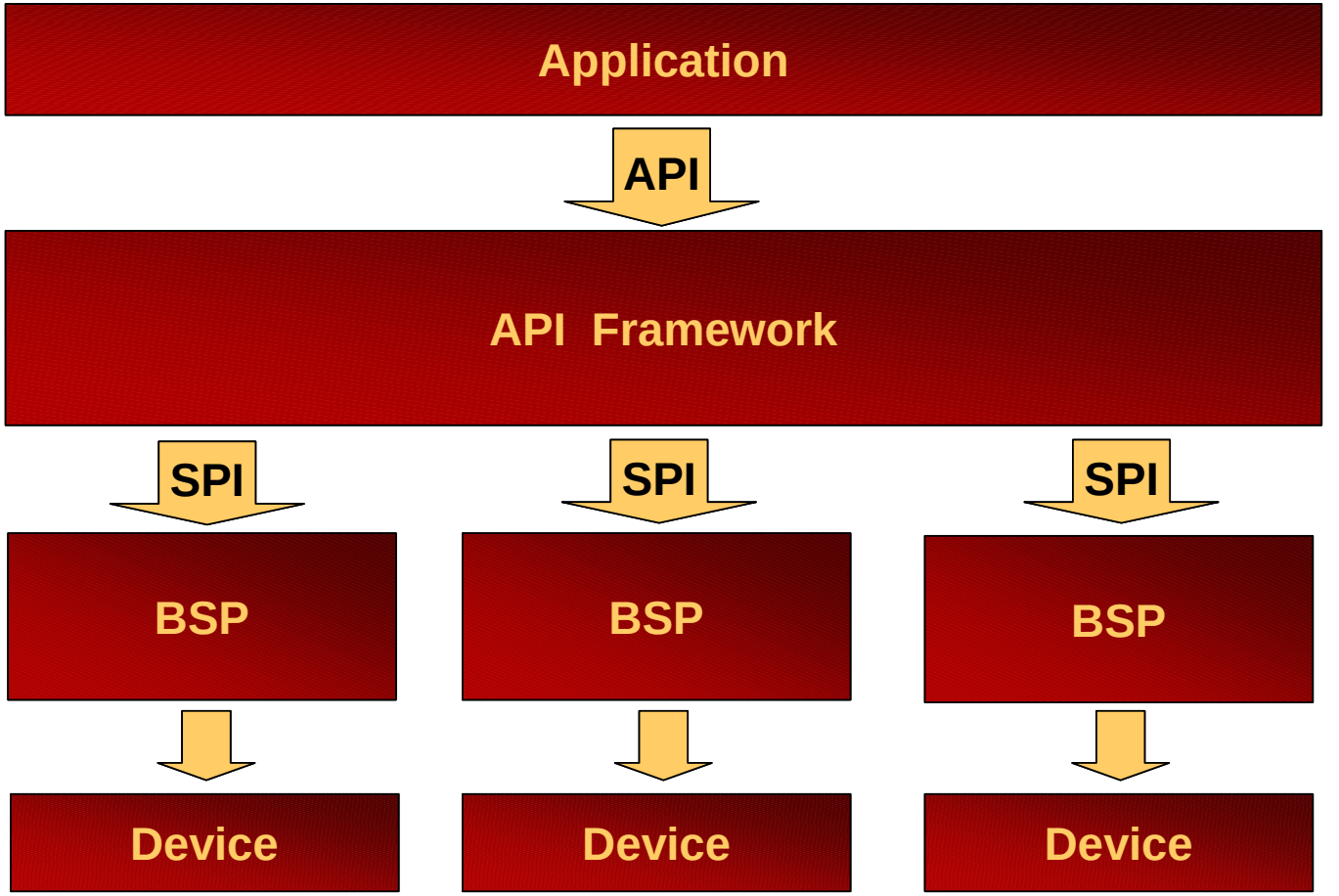
- Define requirements based on architectural scenarios
- Identify alternative architectural approaches to meeting these requirements
- Analyze these alternative approaches
- Select an approach (or combination) that best satisfies the requirements
- Further define/refine the selected approach
- Determine what edits/extensions are required to the BioAPI and GSC-IS to implement the defined approach
- Document the results in a report to M1

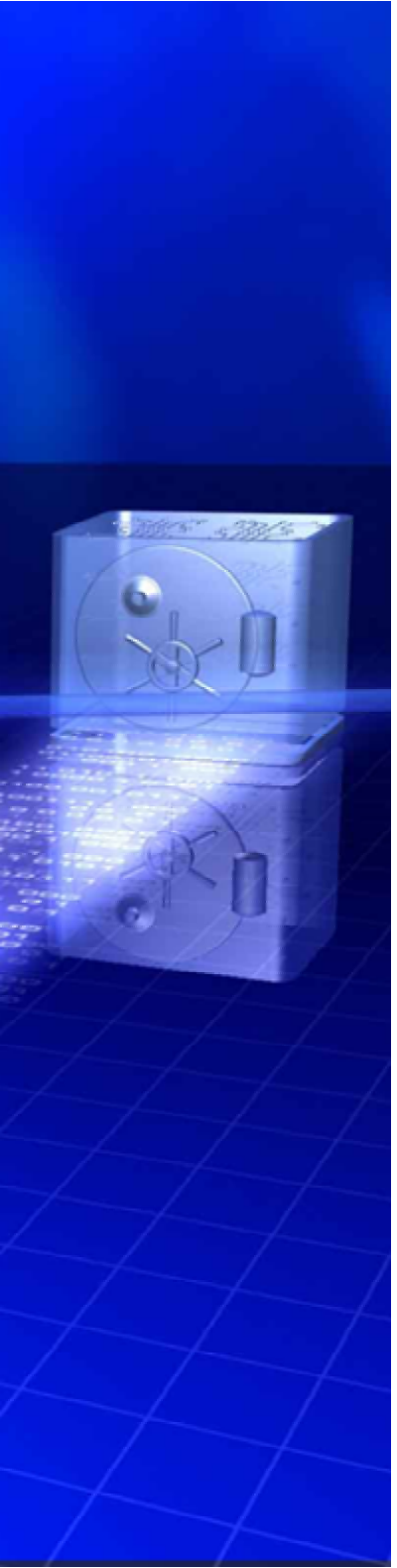
- Constraints:
  - GSC-IS v2.1 in progress and heading to B10 & SC17
  - BioAPI progressing through SC37
  - Users demanding integrated solutions NOW!

GSC-IS Architecture



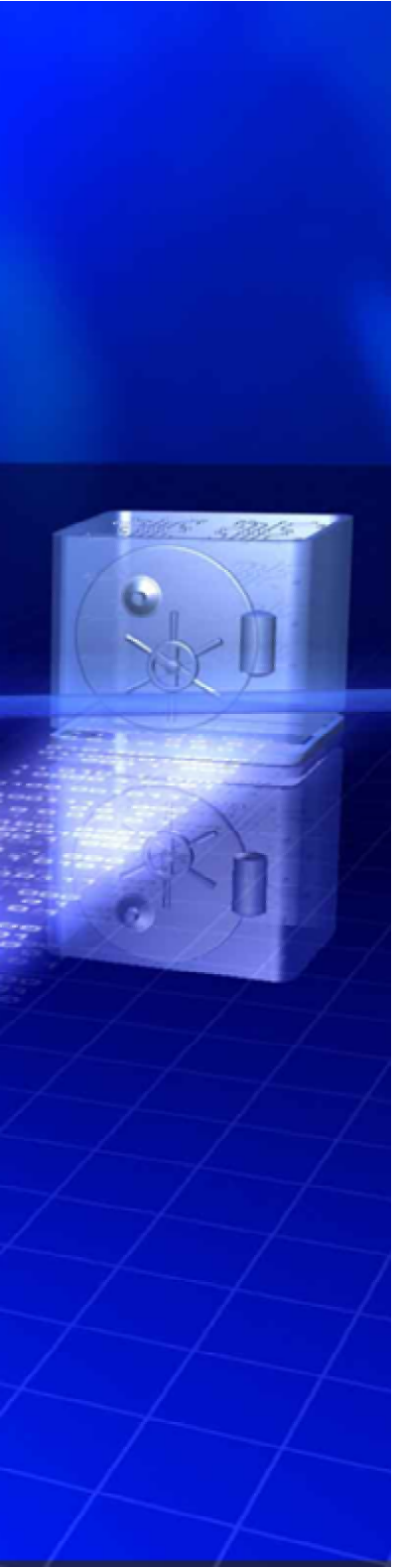
BioAPI Architecture





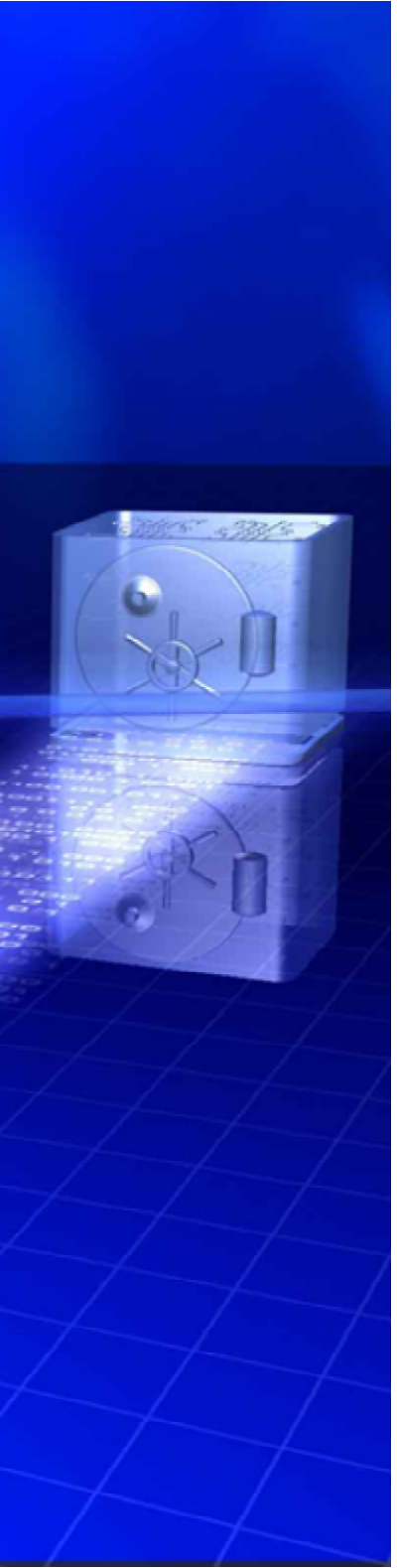
Status

- Requirements baselined at May meeting in Orlando
- AHG requested in Feb that GSC AWG defer inclusion of biometric functionality until study complete
- DMDC submitted proposed approach
- Gap analysis comparing augmented DMDC proposal against baselined requirements at June meeting
- Report slated for publication late August



Summary Requirements

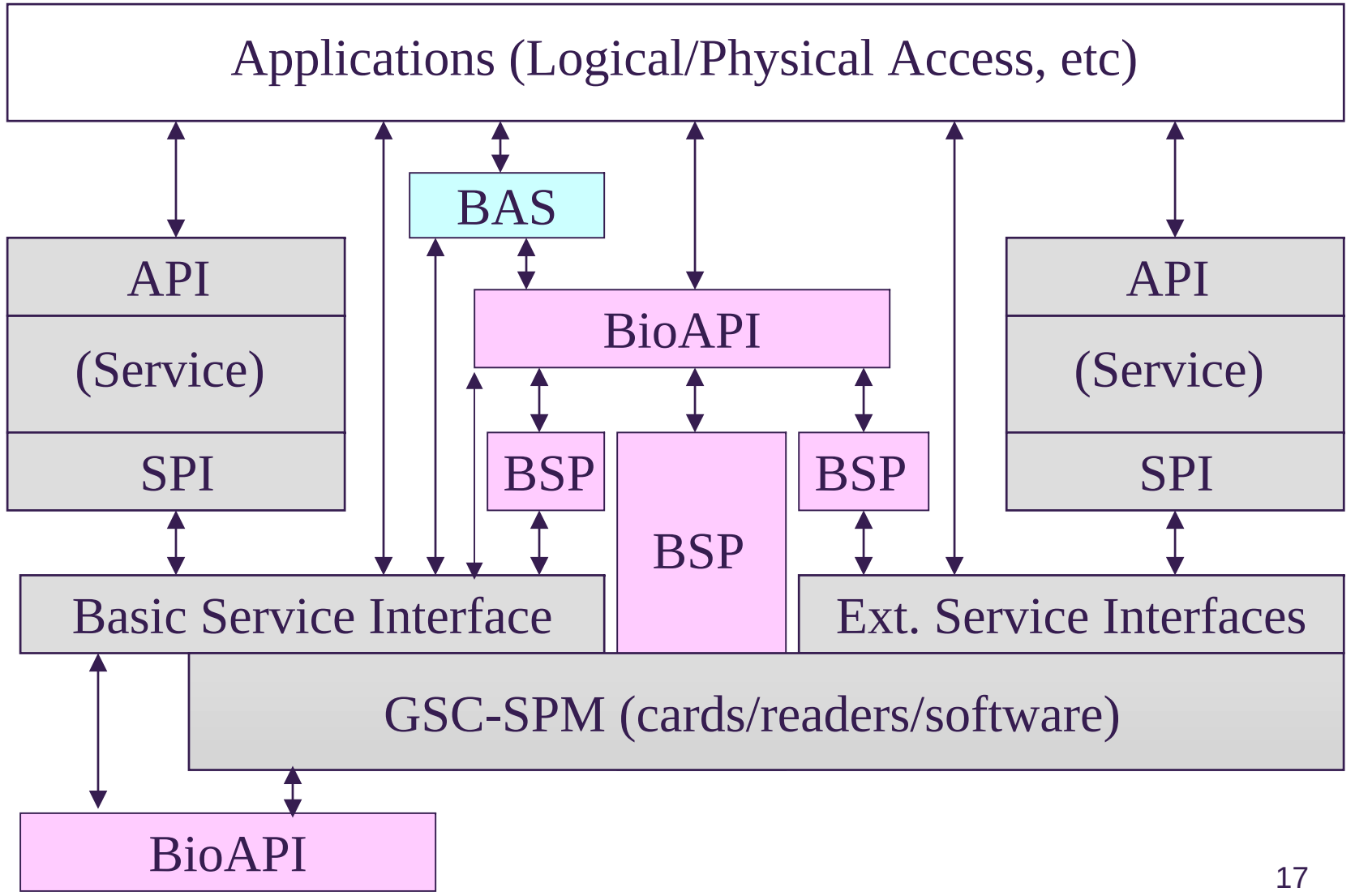
- Top-Level Functions
  - Authentication to Card
  - Off-Card Authentication
- Applications
  - Smart Card Centric
    - e.g., Biometric used for access control to card
  - Biometric Centric
    - e.g., Smartcard used for portable/secure storage of biometric
- Scenarios
  - Store on Card, Match on Host
  - Store on Card, Match in Device
  - Store on Card, Match on Card

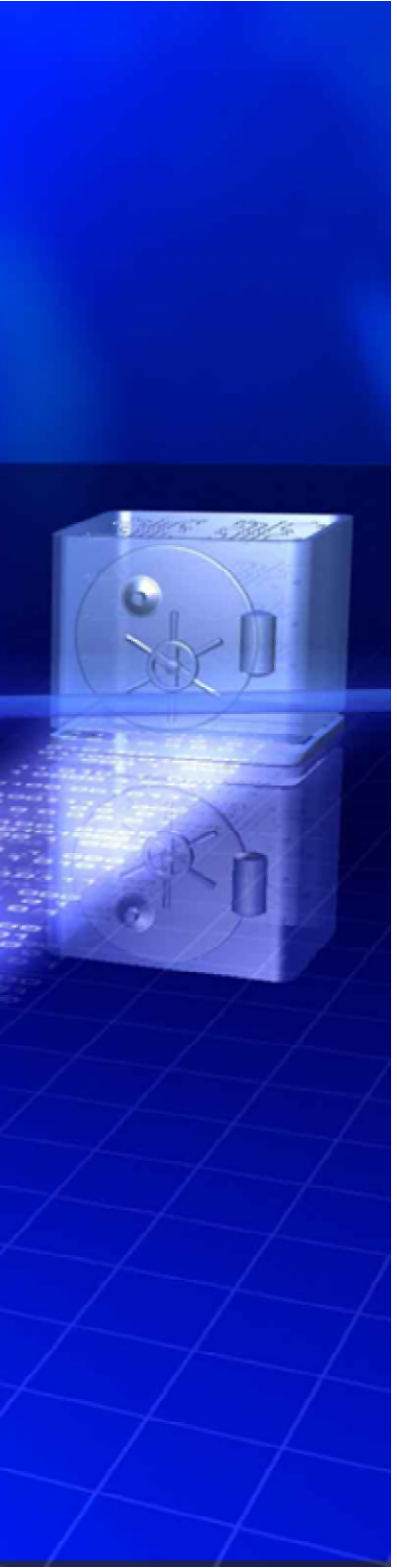


Sample Sub-Requirements

- Differences in storage/protection/accessibility requirements for STOC v. MOC
- Need for directory/discovery mechanism to determine what biometric data is on the card (enrollments)
- Support for enrollment at issuance and post issuance
- Release of “pre-match” data to support external capture/processing of biometric data
- Scoring and thresholding considerations

Architecture Possibilities





More information

- Website: www.incits.org
  - Select Technical Committee M1-Biometrics
  - Go to Document Register
- AHG Baseline requirements: Doc# M1/03-0239
- Next meeting:
  - Aug 18-22, MitreTec – Virginia

- Chair:
  - Fernando Podio
  - 301-975-2947
  - Fernando.podio@nist.gov

- AHG Chair:
  - Cathy Tilton
  - 703-708-9280
  - ctilton@saflink.com