European Commission
United Nations Development Programme
International IDEA

In collaboration with

International Organization for Migration
Canadian International Development Agency
Organization of American States

Procurement of Material for Biometric Voter Registration
Cases of RDC, Togo and Guinée-Conakry

Dunia Ramazani, Ph.D., ICT Election Specialist, EC-UNDP Joint Task Force

Joint Training on
Effective Electoral Assistance
Brussels, 1-5 December 2008

Outline

- Introduction
- Complexity of biometric solutions
- Roles and responsibilities
- Standard compliance
- Acceptance testing of solutions
- Case studies
- Concluding remarks

Complexity

This complexity arises from the intertwining of equipment, software and services requiring careful design of Terms of References (operational concept of registration) with possible implications on total cost of acquisition, operation and storage as well as training issues.

Complexity

Components of biometric solutions include but are not limited to:

- Power source (generator, solar panel, inverter, battery,etc.)
- Photo capture device
- Fingerprint scanner
- Data capture device
- Data storage and transmission
- Data processing (Data centre including ABIS) and printing facilities
- Training
- Operational supervision of the registration process
- Technical support
- Registration software
- Voter list production software
- Mobility
- Standard compliance.

Complexity

Convergence of National ID, Biometric passports and voter cards

ICAO Doc 9303

Electronically enabled machine readable passports, e-Passports / e-MRTDs will include mandatory globally interoperable biometric data which may be used as an input to facial recognition systems and, optionally, to fingerprint or iris recognition systems.

Roles and Responsibilities

Total solutions versus technology transfer to EMB

Total solutions mean the provider controls the process end to end.

Technology transfer to EMB means at the end of the process, the EMB is capable of repeating itself the process without external assistance.

It is not clear at this point how to achieve technology transfer.

Standard compliance

Quality of collected data

Fingerprint and facial images of poor quality result in poor matching performance.

Fingerprint images must be compliant with Fingerprint Image Data Interchange Standard ISO/IEC 19794-4

- WSQ compression at 500 ppi resolution
- 8 bits pixel depth, or 256 gray levels
- Compression to a size no smaller than 1/15 the original size (16.7 Kbytes)
- Images should be no smaller than 320 x 320 pixels in size.

Standard compliance

Quality of collected data

Facial images must be JPEG or JPEG2000.
Facial images be compressed to between 15 and 20 Kbytes in size, and are non-compliant if smaller than 12 Kbytes.

Software shall be able to find eye locations, and also to align, scale, and crop the image, and optimize contrast.

Software shall be used to check the image for potentially non-compliant features, such as yaw, hot spots, shadows, smiles, low brightness and contrast, incorrect image geometry, improper head position, a cluttered background, and poor focus.

Standard compliance

Standard bodies

ISO and IEC have a joint technical committee for information technology standards called JTC1.

In 2002, ISO/IEC JTC1 established a subcommittee to develop generic biometric standards, which was designated as SC37. This subcommittee is composed of six working groups, each addressing a specific area of work:

- WG1 – Harmonized Biometric Vocabulary
- WG2 – Biometric Technical Interfaces
- WG3 – Biometric Data Interchange Formats
- WG4 – Biometric Profiles
- WG5 – Biometric Performance Testing and Reporting
- WG6 – Cross-Jurisdictional and Societal Aspects of Biometrics

Standard compliance

List of biometric standards that have been approved and published:

ISO/IEC (International Organisation for Standardisation)/International Electro-Technical Commission)

- ISO/IEC 19794-2, Information Technology – Biometric Data Interchange Format – Part 2: Finger Minutiae Data
- ISO/IEC 19794-4, Information Technology – Biometric Data Interchange Format – Part 4: Finger Image Data
- ISO/IEC 19794-5, Information Technology – Biometric Data Interchange Format – Part 5: Face Image Data
- ISO/IEC 19794-6, Information Technology – Biometric Data Interchange Format – Part 6: Iris Image Data
- ISO/IEC 7816-11:2004, Identification cards – Integrated circuit cards – Part 11: Personal verification through biometric methods

Standard compliance

ICAO (International Civil Aviation Organisation)

• ICAO Doc 9303, “Machine Readable Travel Documents”, 5th Edition, March 2003 – “Biometrics Deployment of Machine Readable Travel Documents”, Technical Report, Version 2.0, May 21, 2004 – “Machine Readable Travel Documents, Technical Report, Development of a Logical Data Structure – LDS – for Optional Capacity Expansion Technologies”, Technical Report, Version 1.7, May 18, 2004

Standard compliance

INCITS (International Committee for Information Technology Standards)

- ANSI/INCITS 358-2002, “The BioAPI Specification”, February 13, 2002
- ANSI/INCITS 377-2004, “Finger Pattern-Based Format for Data Interchange”, January 23, 2004
- ANSI/INCITS 378-2004, “Finger Minutiae Format for Data Interchange”, February 20, 2004
- INCITS 381-2004, “Finger Image Format for Data Interchange”, May 13, 2004
- ANSI/INCITS 385-2004, “Face Recognition Format for Data Interchange”, May 13, 2004

Standard compliance

INCITS (International Committee for Information Technology Standards)

- ANSI/INCITS 394-2004, “Application Profile for Interoperability, Data Interchange and Data Integrity of Biometric-Based Personal Identification for Border Management”, October 5, 2004
- ANSI/INCITS 395-2005, “Signature/Sign Format (for Data Interchange)”, August 12, 2005
- ANSI/INCITS 396-2005, “Hand Geometry Format for Data Interchange”, May 12, 2005
- ANSI/INCITS 398-2005, “Common Biometric Exchange Formats Framework (CBEFF)”, February 7, 2005

Standard compliance

ANSI (*American National Standards Institute)*

• ANSI X9.84-2003, “Biometric Information Management and Security for the Financial Services Industry”, June 2003
• ANSI/NIST-ITL 1-2000, “Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information”, July 27, 2000

Standard compliance

OASIS (Organization for the Advancement of Structured Information Standards)

1. “XML Common Biometric Format (XCBF)”, Version 1.1, August 2003, Organization for the Advancement of Structured Information Standards

Other

• NISTIR 7151, “Fingerprint Image Quality”, August 19, 2004

• IAFIS-DOC-01078-7, “Electronic Fingerprint Transmission Specification (EFTS)”, Version 7.1, May 2, 2005, Federal Bureau of Investigation, Criminal Justice Information Services Division

2. IAFIS-IC-0010(V3), “Wavelet Scalar Quantization (WSQ) Grayscale Fingerprint Image Compression Specification”, December 19, 1997 (Federal Bureau of Investigation)

Standard compliance

When standard compliance is not mandatory, it may result in difficulties to migrate electoral data (fingerprints and photographs) to other platforms supported by several other vendors.

Some of the standards which need to be taken into consideration are:

- ANSI/TIA-942;
- ACM statewide database of registered voters;
- Voluntary Voting System Guidelines (VVSG);
- ANSI/NIST-ITL 1-2000 standard : Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information - Part 1 (ANSI/NIST-ITL 1-2007);
- BS ISO/IEC 19794.

Acceptance testing

EMBs must follow standard processes for acquiring software products and services (IEEE 12207.0 Standard, entitled *Industry Implementation of International Standard ISO/IEC 12207:1995, Standard for Information Technology, Software Life Cycle Processes*)

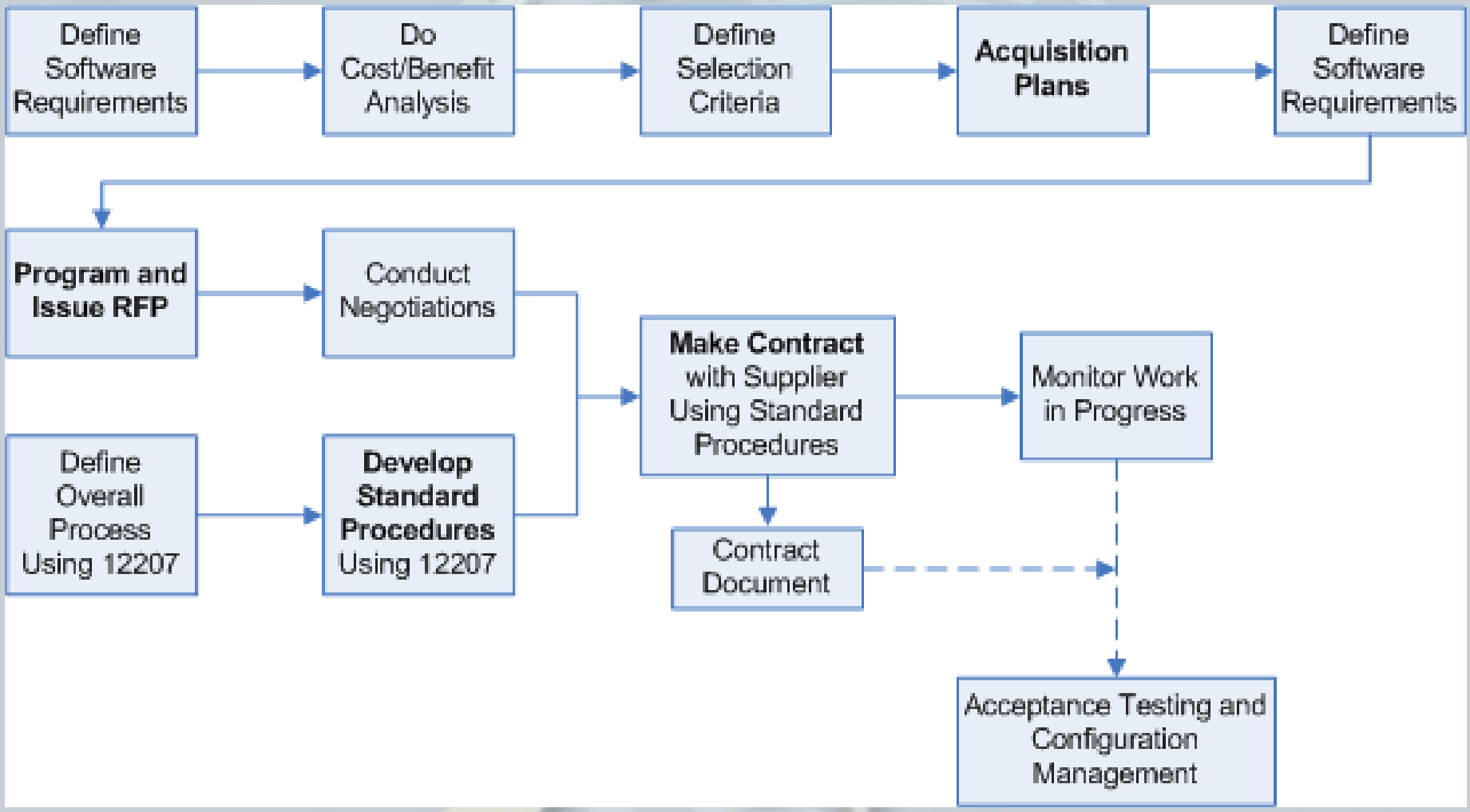
This standard presents the commonly accepted practices for ensuring a well-defined and persistent assurance process for acquired software. The 12207 framework describes a complete set of practices for software, which range all the way from conceptualization through retirement.

Acceptance testing

This translates into:

- Preparing a concept or a need to acquire, develop, or enhance a product or service
- Preparing a set of requirements including relevant design, testing and compliance standards
- Preparing a set of acceptance criteria and criteria for evaluation
- Documenting acquisition requirements depending on acquisition option selected
- Establishing plans for supplier selection
- Performing acceptance reviews and testing

Acceptance testing



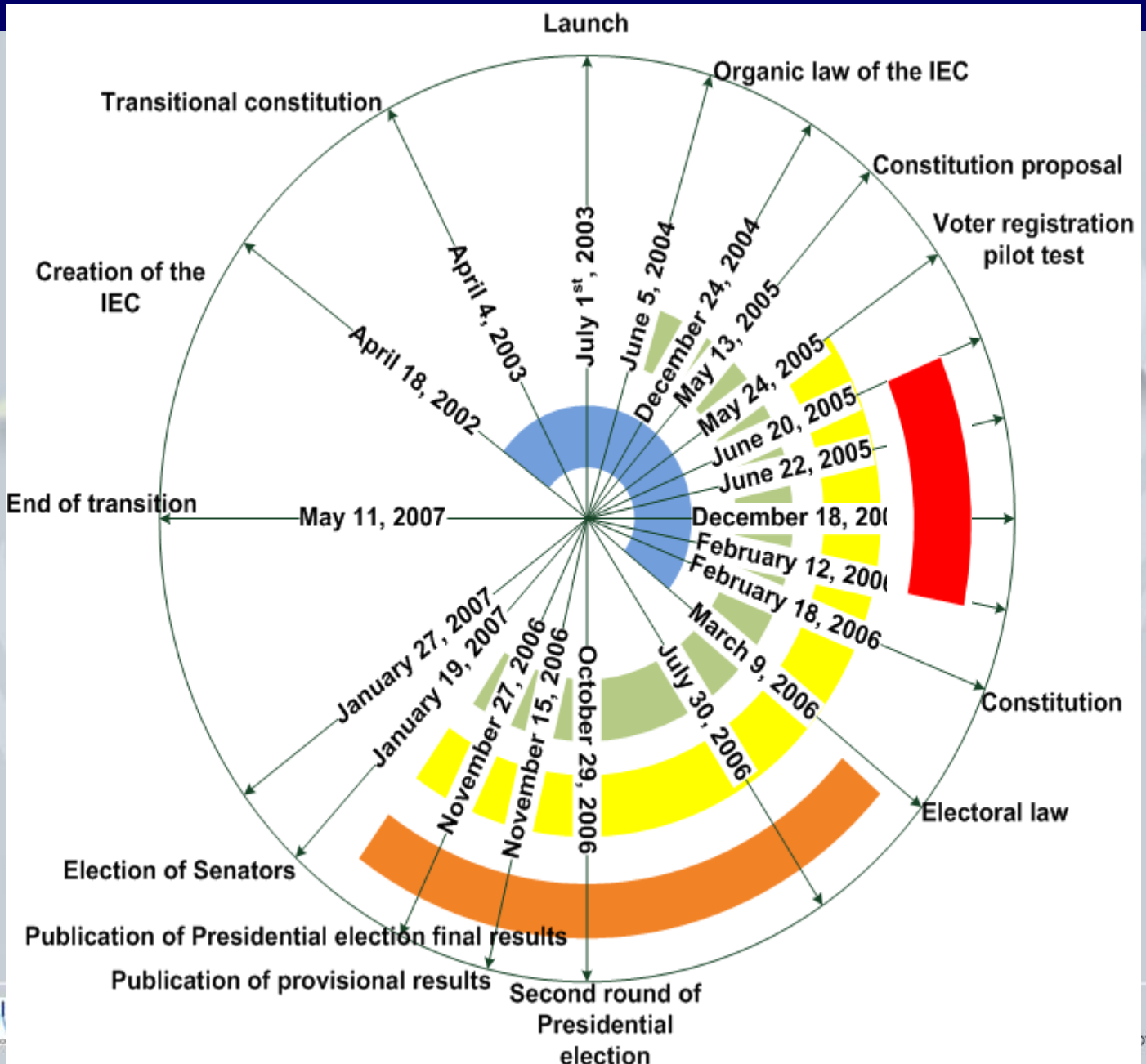
Acceptance testing

More importantly, the RFP has to be both feasible and cost justifiable.

Formal acceptance of the solution includes preparation and performance of test cases, test data, test procedures, and test environment.

Inspections and audits have rigor but they require resources and have concomitant costs.

RDC


Launch
Organic law of the IEC
Constitution proposal
Voter registration pilot test
Constitution
Electoral law
Second round of Presidential election
Publication of provisional results
Publication of Presidential election final results
Election of Senators
End of transition
Creation of the IEC
Transitional constitution
April 18, 2002
April 4, 2003
July 1st, 2003
June 5, 2004
December 24, 2004
May 13, 2005
May 24, 2005
June 20, 2005
June 22, 2005
December 18, 200
February 12, 200
February 18, 2006
March 9, 2006
July 30, 2006
October 29, 2006
November 15, 2006
November 27, 2006
January 19, 2007
January 27, 2007
May 11, 2007


BIC
WHITEBOARD
MARKER

Guinée-Conakry

Absence of the EMB during the development of ToR

- Sustainability issues addressed by the ToR.
- Detailed specifications that included software.
- Preliminary consultations with procurement.
- Insufficient funds.

Concluding remarks

Acquiring biometric solutions is a complex set of activities which require technical expertise, time and financial resources.

Nonetheless, solutions have to be standard compliant to avoid EMB being taken hostage by some vendors.

Given the financial resources committed, best value for money means assurance quality and formal acceptance of the solution. This requires careful design of software specification documents including test cases, test data, test procedures and test environment as well as timing of such acceptance.