Regional Biometric Data Exchange Solution (RBDES)

Q: What is the RBDES?

RBDES is a multinational tool providing a data sharing framework and a technical secure communication interface; consisting of legal, technical, privacy and business processes. RBDES will allow Bali Process members to share data with any other country that they have implemented the necessary bilateral arrangements with.

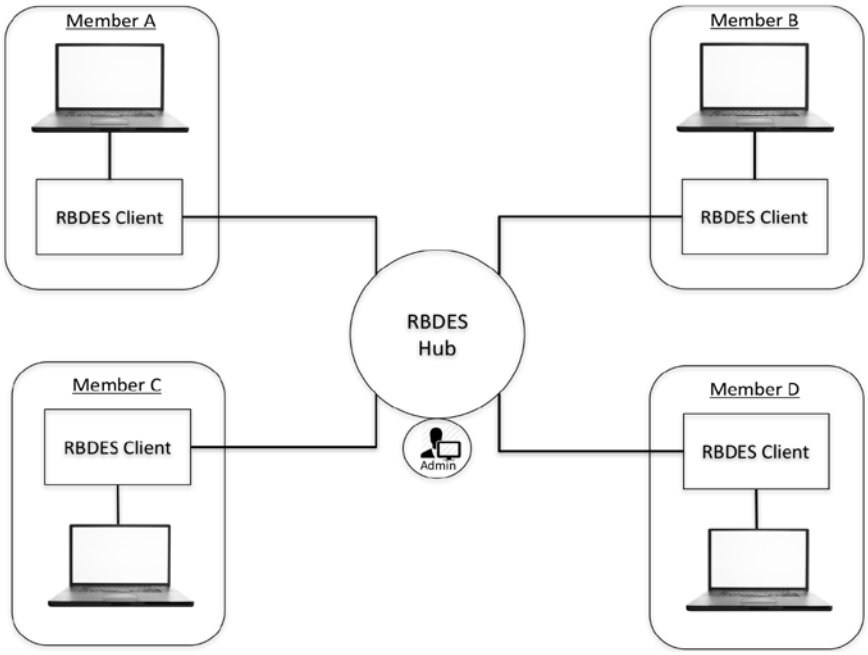
For a brief overview of RBDES please view the video brochure at the below link: https://www.dropbox.com/s/tf4scnlaq04rx3l/AV0.mp4?dl=0

Q: How has the RBDES been built?

The key function of RBDES is to allow Bali Process members to connect securely via the internet and transmit data (fingerprint biometrics) from one endpoint (requesting client), through the Hub (the RBDES central infrastructure, router) to the second endpoint (receiving client).

The clients will provide users with a mechanism for both sending and receiving messages to the RBDES Hub. The Hub provides the necessary functionality to connect members, and records all relevant transactional and access data for the purposes of auditing and reporting.

The diagram below outlines the Hub and Client concept:



Q: Is RBDES connected to national databases, for example the Border Management Information System?

No the RBDES is not connected to national databases or information systems, it also isn't a database itself and doesn't replace existing systems. The RBDES is a secure tool designed to facilitate data sharing amongst Bali Process members; once Participating Members receive a request they will be required to manually confirm the data against their existing information systems.

However, the RBDES is built on open standards technology meaning that integration with existing systems is possible with minimal cost. Integration may remove some of the manual processing required by users.

Membership

Q: Who do we contact to discuss membership?

To discuss joining RBDES or for any RBDES questions you can contact the International Organization for Migration (IOM). Please email RBDES@iom.int

In the near future the Bali Process Regional Support Office (RSO) will also complete the recruitment of the RBDES Manager role – this role will be a central contact point for members with queries regarding RBDES, further details will be provided once the RBDES Manager is identified.

Q: What costs are involved?

Ongoing cost details are currently being finalized and a final cost structure will be determined by the RBDES Oversight Committee. The Oversight Committee will comprise of 1 representative from 5 Bali Process members (on a two-year rotational basis) and the RBDES Manager (with no voting rights).

There will be a one-off establishment fee for Participating Members and a license fee (based on transaction volumes) on an ongoing basis.
Due to the nature of the system architecture there will be economies of scale as the number of Participating Members increase.

RBDES fees will be coordinated through the RBDES Oversight Committee and managed by IOM.

The first five Participating Members to make use of the system will receive the required RBDES hardware, purchased for the kick-off workshop, free of charge.

Q: Who provides the governance?

The **National Accountability Officer** (Local Administrators) is an official formally designated by each Participating Member in the Associated Arrangements. The National Accountability Officer will be responsible for the operation of the Participating Member's systems and processes in a way that is consistent with the Policy Framework. Users of the System will be trained on the use of the System and its safeguards.

The **RBDES Manager** will manage member participation in the RBDES. The RBDES Manager will continue to promote the use and the development of the RBDES, and explore any opportunities to provide training and assistance to the Bali Process membership. The RBDES Manager will also provide administrative assistance to the Oversight Committee, report on the System at Bali Process' meetings and act as a non-voting member of the Oversight Committee.

The **System Administrator** will manage the technical operation of the System. The System Administrator's responsibilities are outlined in the Service Arrangements contained in the Terms of Use. These responsibilities include user management, handling of technical issues, reporting, managing business rules and making emergency technical changes to the System.

The **Oversight Committee** is a collective body that will govern the ongoing implementation and operation of the RBDES. The Oversight Committee will comprise of 1 representative from 5 Bali Process members (on a two-year rotational basis) and the RBDES Manager (with no voting rights). The Oversight Committee's responsibilities are outlined in a Terms of Use and Terms of Reference. The Oversight Committee's responsibilities include reviewing the operations of the RBDES, reviewing any communications, incident reports or any other reports from the RBDES Manager and

System Administrator, and discussing any concerns, improvements, amendments to the RBDES. The Oversight Committee may suspend or terminate a member's participation if there has been any breach.

The **Bali Process Ad Hoc Group Senior Officials** will be responsible for raising any objections to amendments to the RBDES recommended by the Oversight Committee.

Q: Where can I access the RBDES Policy Framework?

The policy information for RBDES is contained in the *Policy Framework for the Regional Biometric Data Exchange Solution.*
You can access the policy framework at: http://www.baliprocess.net/regional-support-office/regional-biometric-data-exchange-solution/

Q: How can we benefit from using the RBDES?

The RBDES will enhance Participating Members' decision making in relation to border management and migration processes. RBDES can link Participating Members with other Participating Members who may have relevant and valuable information that can be used to verify an individual's identity. The System is a simple and user friendly channel for communication used to securely connect members over the Internet.

Q: What are the responsibilities of members?

Participating Members will be responsible for negotiating and entering into Associated Arrangements, training users of the System and other officials, conducting privacy impact assessments, and ensuring the security of their domestic systems.

By participating in the RBDES, Participating Members will comply with the Framework, in particular the human rights and privacy safeguards provided under the Framework. While the RBDES is based on principles of regional cooperation, collective responsibility and burden sharing, once data is exchanged, each Participating Member will be responsible for any decisions or actions that they take.

Biometrics

Q: What biometrics can be exchanged with RBDES?

The current system is configured to support exchanges of fingerprints only.
However, the system has the potential to support any data sharing according to specific Associated Agreements to be agreed bilaterally or multilaterally between Participating Members.

Q: Will RBDES support other biometrics?

In the future the system could support any type of data that Participating Members may want to securely share, for example other biometrics; iris, DNA, or biographic details. This will involve some system configurations and will be discussed with Participating Members as required.

Q: How are biometrics uploaded to the RBDES?

Using the RBDES upload function, within the user interface, the designated user will attach the biometric file/s to the message before sharing it with the receiving Participating Member.

RBDES is not a database of biometric information, therefore users will need to access their local system to capture biometrics before uploading the file.

Q: What information can be sent through RBDES?

RBDES can share any information specified in the relevant Associated Agreements to be agreed by the Participating Members bilaterally and/or multilaterally. The current system can send:

- Message Identifier (system generated)
- Message Reference (optional)
- Priority
- Biometric file (fingerprint).

Q: What type of reply can be sent via RBDES?

Currently the RBDES is configured to return the following messages:
Match, No Match or Error

- Match – in the case of positive match with national databases
  - Biographics (optional): in case of positive match with national databases, the full identification of the person can be shared (Name, Nationality, Date of Birth, Passport Number)
- No Match – in the case where there are no matching details in the national databases
- Error Type (if an Error occurs in the verification process, for example due to the low quality of the image shared)

Q: What if a potential Participating Member does not currently have suitable equipment to collect biometric data?

There are a number of affordable options that may be considered for biometric enrolment and matching. An Ad hoc needs assessment can be requested to the RBDES Manager and/or to the System Administrator. Tailored solutions may be considered, including the IOM developed VERIFIER TD&B. You can learn more about the VERIFEIR system by contacting the IOM.

Q: Could the RBDES be connected to an automated response biometric identification system?

The RBDES could be connected to an automated response biometric identification system. The RBDES is built on open standards technology meaning that integration with existing systems is possible with minimal cost.

Q: What if designated users need specific training related to biometrics?

Please contact the IOM and options can be coordinated with the RBDES Manager.

RBDES Operations

Q: What are the possible uses of the RBDES?

Potential use cases for the confirmation of identity through the RBDES include:

- Undertake checks to facilitate family reunification requests from a Non-Government Organization (NGO)
- Assist in speeding up registration process for enrolment into the United Nations High Commissioner for Refugees (UNHCR) system
- Migrant worker registration
- Irregular movement of people (returns)
- Labour migration
- Emergency repatriation
- Resettlement
- Re-trafficking

This is not an exhaustive list of potential, if you believe that the RBDES could be of use please contact IOM at RBDES@iom.int

Q: Who can be contacted if support is needed?

Please contact the IOM at RBDES@iom.int

Q: How quickly will the RBDES respond to a request?

A number of factors may affect the system's speed and response including – user workload and network connectivity. If in doubt, please contact the IOM at RBDES@iom.int

It is important to note that the RBDES is not an automated response system. An officer of the receiving member must download the biometric file for comparison to national databases and systems before replying to the requestor. While the system will exchange the data within seconds additional time is required for matching against systems not integrated with RBDES.

During negotiations of Associated Agreements participants can decide on mutually agreeable response times.

Q: What equipment is needed for the RBDES?

Upon joining each Participating Member will be provided with a specialized machine (computer) that has everything needed to connect to the RBDES and share data.

In order to process requests (sent or received) the Participating Member will need access to their national biometric databases or systems (biometric matching capability) not integrated with RBDES.

Q: Who is responsible for user setup and management?

The IOM is responsible for all user setup and management. For more information, please contact RBDES@iom.int

Security

Q: Where is the biometric data stored?

Biometric data is only stored temporarily on the recipient client (computer) prior to a response being sent. After a response is successfully sent the biometric data is deleted. Biometric data is not stored through the hub for longer that it takes to deliver the message (the message expiry time is set to 30 seconds).

Q: How secure is the data shared with the RBDES?

Security is central to the design of every aspect of the RBDES. All data is encrypted end-to-end through a secure Virtual Private Network (VPN). A VPN enables users to send and receive data across shared or public networks (i.e. the internet) as if their computing devices were directly connected to the private network. Messages can only be decrypted by the intended recipient, and remain encrypted through the transmission process.

All actions within the RBDES are recorded through transaction logs and can be audited or reviewed and reported on as required.

Q: Is it possible for anyone else to read the data that is shared with a partner?

The data is encrypted using the receiving partner's public key, the process is one to one. This means that even if other security measures such as the VPN and access control were circumvented the message could not be accessed without the receiving partner's private key. The messages are only decrypted when the user requests to take it external to the system for matching.

Q: What are the security measures in place with RBDES?

RBDES contains multiple inbuilt security controls, specifically the following:

- Role-based user access to the RBDES client.
- Logical segregation of components handling unencrypted data from those handling only encrypted sensitive data.
- RBDES clients and the central hub infrastructure are locked down by the use of a hardened virtual machine (VM), the machine cannot access 'outside' environments or apps.
- Segregation of the communication channel between clients and the Hub by means of a VPN.
- Clients must be explicitly authorised via external procedures to gain access credentials to the VPN.
- VPN credentials locked to an IP-address and physical hardware.
- Encryption of request and response messages via Private Key Infrastructure (PKI) encryption. (A public key infrastructure (PKI) supports the distribution and identification of public encryption keys, enabling users and computers to both securely exchange data over networks such as the Internet and verify the identity of the other party.)
- Centralised distribution of public keys via trusted distribution mechanisms.
- Ability to revoke decryption keys.
- Audit logging on all transactions.

Q: Is there additional documentation related to the security of the RBDES?

There is a suite of technical documentation that includes a System Security Plan, a System Risk Management Plan, a System Engineering Management Plan and a System Architecture Design.

Please contact IOM at RBDES@iom.int should you wish to review these documents.

Q: If there is a suspected private key stolen how will this be handled?

In the system the National Accountability Officer can trigger key revocation. The System Administrator must be immediately notified. Details of how to revoke a key are provided in the RBDES Local Administrator Manual.

Q: Is data stored in the hub or is there a central database?

No personal identifiable information, biometrics or biographics are stored in the RBDES hub or the members individual clients. Only transactional data is at rest in the hub, that is the time stamps of messages sent and received, message reference numbers etc.