



**BANKSERVAFRICA**



# **BANKSERVAFRICA AUTOMATED TRANSMISSION SERVICE (AXS)**

**VERSION 7.8 – JULY 2023**



**COPYRIGHT RESERVED – A BANKSERVAFRICA GROUP PUBLICATION**

The information contained in this document is proprietary information which is protected by copyright and at law. All rights are reserved. No part of the information contained in this document may be copied, reproduced, disseminated, transmitted, transcribed, extracted, stored in a retrieval system or translated into any language in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, in whole or in part, without the prior written consent of BankservAfrica.

The information contained herein is confidential to BankservAfrica and may not be used or disclosed. Any unauthorised reproduction or disclosure of the information contained in this document will constitute a breach of intellectual property rights and copyright infringement, and may result in damages to BankservAfrica and render the person liable under both civil and criminal law.

Although every care is taken to ensure the accuracy of this presentation, BankservAfrica, the authors, editors, publishers and printers do not accept responsibility for any act, omission, loss, damage or the consequences thereof occasioned by the reliance by any person upon the contents hereof.

©South African Bankers Services Company Proprietary Limited  
PO Box 62443, Marshalltown, 2107  
Tel: +27 11 497 4000 / Fax: +27 11 493 0595



# CONTENTS

- 1. OVERVIEW OF THE AXS Transmission system ..... 7
  - 1.1. AXS INPUT ..... 7
  - 1.2. FUNCTIONAL OVERVIEW ..... 7
- 2. Application interface for 8 character file names ..... 9
  - 2.1. APPLICATION PROTOCOLS ..... 9
  - DATA FILES ..... 11
  - EXAMPLE OF SERVICES ..... 12
- 3. FILE NAMING CONVENTION FOR 8 CHARACTER FILENAMES ..... 14
  - 3.1. REQUIREMENTS ..... 14
- 4. FILE FORMAT FOR 8 CHARACTER FILENAMES ..... 21
  - 4.1. 01 CONTROL RECORD ..... 21
  - 4.2. DATA RECORDS ..... 22
  - 4.3. 99 END OF FILE RECORD ..... 22
  - 4.4. TRANSMISSION CONTROL FILE – START OF DAY ..... 23
  - 4.5. TRANSMISSION CONTROL FILE – END OF DAY ..... 24
  - 4.6. TRANSMISSION CONTROL FILE – ACK/ NACK FILE ..... 25
- 5. OVERVIEW OF XML (ISO20022) TRANSMISSION SYSTEM ..... 28
  - 5.1. XML INPUT ..... 28
  - 5.2. XML FUNCTIONAL OVERVIEW ..... 28
- 6. APPLICATION INTERFACE FOR XML (ISO20022) FILES ..... 30
  - 6.1. APPLICATION PROTOCOLS ..... 30
  - 6.2. EXAMPLE OF SERVICES ..... 32
  - 6.3. XML TRANSMISSION FILE SIZES ..... 33
  - 6.4. XML SUBSERVICES FOR AUTHENTICATED COLLECTIONS ..... 34
- 7. AXS SECURITY PROCESS FOR EIGHT CHARACTER FILENAMES ..... 35
  - 7.1. PLAYERS IN THE AUTHENTICATION PROCESS ..... 35
  - 7.2. TECHNIQUE ..... 35
  - 7.3. EXCHANGE OF KEYS ..... 35
  - 7.4. PROCESS ..... 35
  - 7.5. SECURITY PROCESS FOR XML (ISO20022) FILES ..... 36
- 8. COMPRESSION METHODS ..... 39
  - 8.1. FILE COMPRESSION ..... 39
  - 8.2. APPLICATION PROTOCOL COMPRESSION ..... 39
  - XCOM: CATERS FOR APPLICATION PROTOCOL COMPRESSION. .... 39
- 9. FILE TRANSFER PROTOCOLS ..... 39



LIST OF FIGURES

Figure 1: File layout..... 11

Figure 2: Example of an inward transmission to BankservAfrica..... 12

Figure 3: Example of an outward transmission with settlement from BankservAfrica ..... 13

Figure 4: Transmission message types ..... 31

Figure 5: Example of inward transmission to BankservAfrica ..... 32

Figure 6: Outward transmission service from BankservAfrica..... 32

LIST OF TABLES

Table 1: Transmission service data streams ..... 9

Table 2: Data flow example ..... 10

Table 3: Application Identifiers ..... 14

Table 4: AVS Sub Application Identifier ..... 15

Table 5: DMCS Sub Application Identifier ..... 15

Table 6: EFT Sub Application Identifiers ..... 16

Table 7: NREG Sub Application Identifiers ..... 16

Table 8: ICMS Sub Application Identifiers ..... 16

Table 9: RTC Sub Application Identifiers ..... 17

Table 10: SASW Sub Application Identifiers..... 17

Table 11: Settlement Report Sub Application Identifiers ..... 18

Table 12: Card Listing Sub Application Identifiers ..... 19

Table 13: File numbering ..... 19

Table 14: File types ..... 20

Table 15: Control record ..... 21

Table 16: End of file Record ..... 22

Table 17: Start of day file..... 23

Table 18: End of day file ..... 24

Table 19: ACK/ NACK File..... 25

Table 20: Control record error codes ..... 26

Table 21: End of file record error codes ..... 26

Table 22: End of day file error codes ..... 27

Table 23: Physical file error codes ..... 27

Table 24: XML Data flow ..... 30

Table 25: XML Subservices for Authenticated Collections ..... 34

CHANGE CONTROL




Version	Date	Description	Author
6.0	13/06/16	Include Authenticated Collections (ISO20022)	K Singh
6.1	04/10/16	AC subservice changes	K Singh
6.2	01/11/16	Remove RVINP and ST001 subservice from AC service	K Singh

7.0	10/11/16	Amend 99 record to cater for 32 bit encrypted working key.	K Singh
7.1	24/05/17	Amend Settlement service to include AuthColl	K Singh
7.2	06/07/18	Included System Error corrections subservices	K Singh
7.3	30/07/18	Include Card Listing	K Singh
7.4	18/09/18	Amended 7.4.2 to remove key length confusion	M de Jager
7.5	09/10/18	Amended 7.4.2 to add hash total padding	M de Jager
7.6	13/08/19	Amended 3.1 – Table 7 for EFT – added CMAFATF	K Singh
7.7	23/06/22	Amended 3.1 – Table 13 for SETT – added SETTREPS; Removed CLC table	K Leshomo
7.8	18/07/23	Amended table of contents to remove CLC; AEDO Amended table 14: File Numbering, rectified the numbering Removed reference to AEDO service	K Leshomo

## GLOSSARY

Term / abbreviation	Definition
AC	Authenticated collections
AVS	Account Verification Service
AXS	Automated Transmission Service
CIS	Central information system
DES	Data Encryption Standard
DMCS	Dual Message Clearing & Settlement
EFT	Electronic funds transfer
ICMS	Integrated Cash Management System
ISDN	Integrated Services Digital Network
LMK	Local Master Key
MAC	Message authentication code
MPLS	Multiprotocol Label Switching
RTC	Real Time Clearing
SETT	Settlement
TMK	Terminal Master Key
ZMK	Zone Master Key
SASW	Saswitch
SWIFT	Society for Worldwide Interbank Financial Telecommunications

**Document Sign-off**

Acceptance			
Kaone Leshomo	Delivery Team Lead	 <small>Kaone Leshomo kaone@bankservafrika.com 2023/08/18 12:08:40 (UTC+2)</small> <b>Signature</b>	
Full Name	Role	Signature	Date
Jeremy Mahabeer	Manager Delivery and Web	 <small>Jeremy Mahabeer jeremy@bankservafrika.com 2023/08/18 12:28:47 (UTC+2)</small> <b>Signature</b>	
Full Name	Role	Signature	Date
Keegan Singh	Head of Applications	 <small>Keegan Singh keegans@bankservafrika.com 2023/08/18 12:29:13 (UTC+2)</small> <b>Signature</b>	
Full Name	Role	Signature	Date
Full Name	Role	Signature	Date
Full Name	Role	Signature	Date



# 1. OVERVIEW OF THE AXS TRANSMISSION SYSTEM

## 1.1. AXS INPUT

- The Automated Transmission Service, (AXS) enables participants to connect directly to the central processing centre for electronic submission and receipt of financial and non-financial data.
- Data is to be submitted electronically in the formats specified in Chapters 2 & 3 – Application Interface. A reply file will be returned to the participant on successful transmission. The reply file can be either an acknowledgment indicating that the file has been accepted for further validation, or it could be a negative acknowledgment indicating that the file has been rejected. An error code will be included to explain the reason for the rejection.
- Participants may connect to the system in the following ways:
  - ✓ SDLC (Diginet Leased Line)
  - ✓ ISDN
  - ✓ MPLS
- AXS provides the following additional features:
  - ✓ Automatic Error Recovery
  - ✓ Data Compression

## 1.2. FUNCTIONAL OVERVIEW

A typical inward file transfer from the participant to BankservAfrica will function as follows:

- A TCP/IP session must be established with BankservAfrica if one does not already exist.
- A file transfer session must be initiated from the participant's transmission platform to BankservAfrica's transmission Platform.
- Upon receipt of each complete file on BankservAfrica's transmission platform, the file(s) will be validated according to the validation procedures for the appropriate service. The service is determined from the file's external name. Data integrity and authenticity of the originator will also be checked, as well as whether each file was received within the specified time window for the service involved.
- Should a file fail the validation checks, the file will be renamed, and a negative online acknowledgement file will be returned to the user, specifying the reason a particular file was rejected. The rejected file will not be returned to the participant.
- If a file passes the validation checks, it will be transferred to the destination system for immediate processing.



A typical outward file transfer from BankservAfrica to the participant will be as follows:

- BankservAfrica's transmission platform will establish a TCP/IP session with the participant's transmission platform, if one does not already exist.
- An AXS file transfer session is then initiated to transfer files, from BankservAfrica's transmission platform to the destination transmission platform
- Upon receipt of each complete file from the transmission platform, the file(s) must be validated according to the validation procedures for the appropriate service. The service is determined from the file's external name. Data integrity and authenticity of the originator must also be checked.
- Should a file fail the validation checks, the file must be renamed or deleted, and a negative acknowledgement file must be returned to BankservAfrica, specifying the reason a particular file was rejected.
- If a file passes the validation checks, it should be transferred to the destination system for immediate processing.





## 2. APPLICATION INTERFACE FOR 8 CHARACTER FILE NAMES

### 2.1. APPLICATION PROTOCOLS

#### 2.1.1. INTRODUCTION

This section specifies the Application level protocols for the AXS transmission platform between BankservAfrica and its users. The primary purpose of these application-level protocols is to authenticate and ensure the integrity of the data. The transmission service will support the following data streams:

Table 1: Transmission service data streams

SERVICE	INWARD	OUTWARD
EFT	X	X
CARD	X	X
ICMS	X	X
RTC		X
CIS		X
SETT		X
AVS	X	X
SASW		X
HCRD	X	X

#### 2.1.2. PROPOSED PROTOCOLS

This specification is based on the assumption that: -

- ✓ The sender is in control
- ✓ The sender is responsible for delivery.

The code set is: -

- Transmission
  - Input to BankservAfrica – ASCII
  - Output from BankservAfrica – ASCII

The flow of data is best described by means of the following table:

### DATA FLOW EXAMPLE

Table 2: Data flow example

SENDER		RECEIVER
Begin-of day-Service -----> (Check if other party is up and running)		<-----Begin-of-day-Service Ack (Go ahead, I am up and running)
	<b>or</b>	<-----Begin-of-day-Service Nack (Error - begin of day)
Send Data File 1-----> (File containing control record, data and end-of-file record)		<-----Receiver Ack file 1 (Receiver pre-validate and accepts)
	<b>or</b>	<-----Receiver Nack file 1 (Receiver pre-validate and rejects)
Send Data File 2 -----> (File containing control record, data and end-of-file record)		<-----Receiver Ack file 2 (Receiver pre-validate and accepts)
	<b>or</b>	<-----Receiver Nack file 2 (Receiver pre-validate and rejects)
Send Data File 3 -----> (File containing control record, data and end-of-file record)		<-----Receiver Ack file 3 (Receiver pre-validate and accepts)
	<b>or</b>	<-----Receiver Nack file 3 (Receiver pre-validate and rejects)
End of day – Service -----> (Once all files have been acknowledged for the service)		<-----End of day - Service Ack (Receiver checks the days transmission for the specific service)
	<b>or</b>	<-----End of day - Service Nack (Receiver checks the days transmission for the specific service)

### 2.1.3. VALIDATION

The following validation procedures have to be in place: -

- Once all the files have been transmitted and acknowledged, an end of day file is transmitted (from the sender). This file will contain controls for the day.

Specific validation procedures are defined for each of the service types.

#### 2.1.4. FILE LAYOUT

The first record on every file will be a control record. This record contains control fields relating to the data in the file, as detailed below. The last record is an end-of-file record.

Different file types are categorised by their content. There are currently two defined categories of files, as indicated in Figure 1 below. The first type is a data file containing a control record, transactions, and an end-of-file record. The other type is a transmission control file containing a control record.

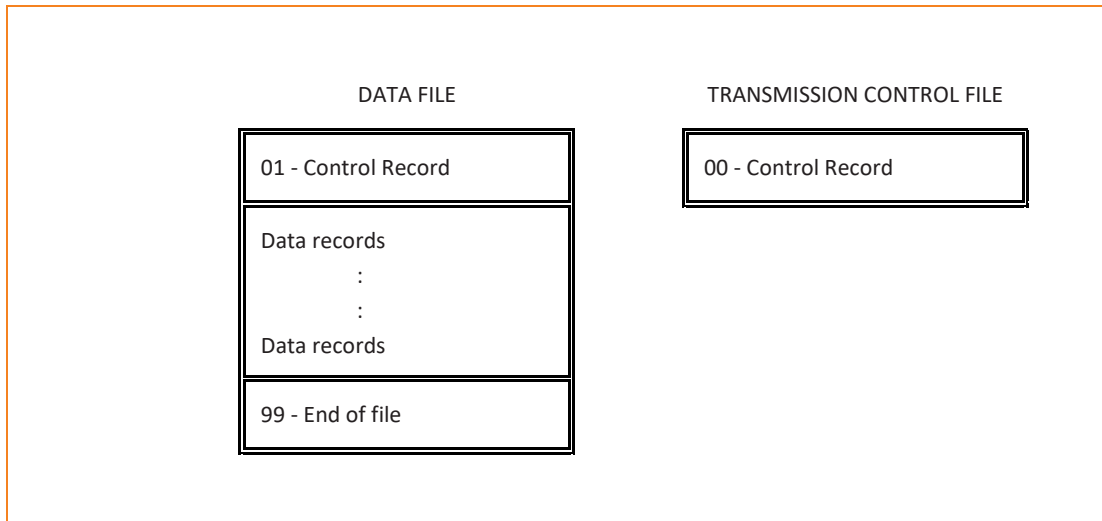


Figure 1: File layout

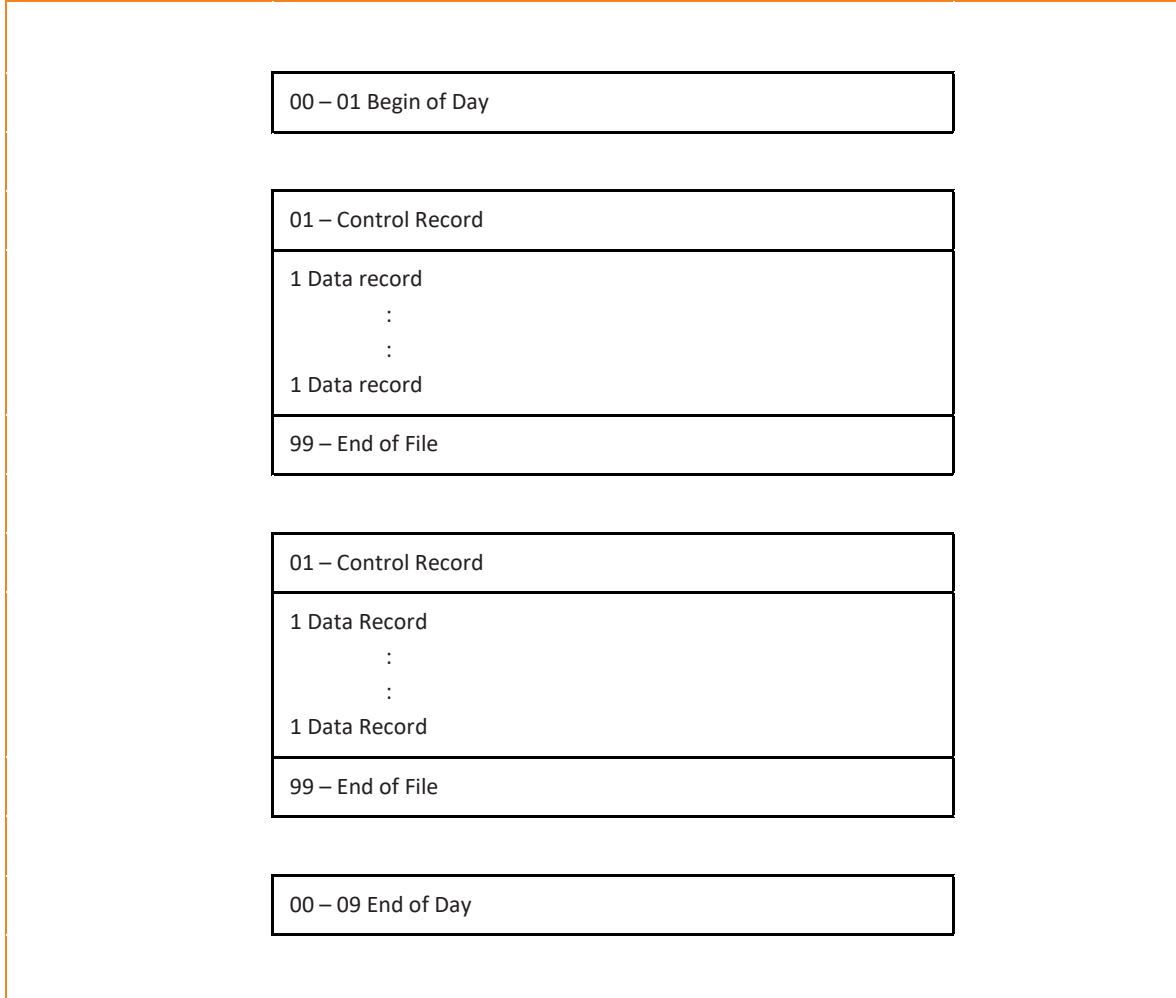
### DATA FILES

The data files will always contain the following:

- One control record (01);
- Multiple data records; and
- One end-of-file record (99).

## EXAMPLE OF SERVICES

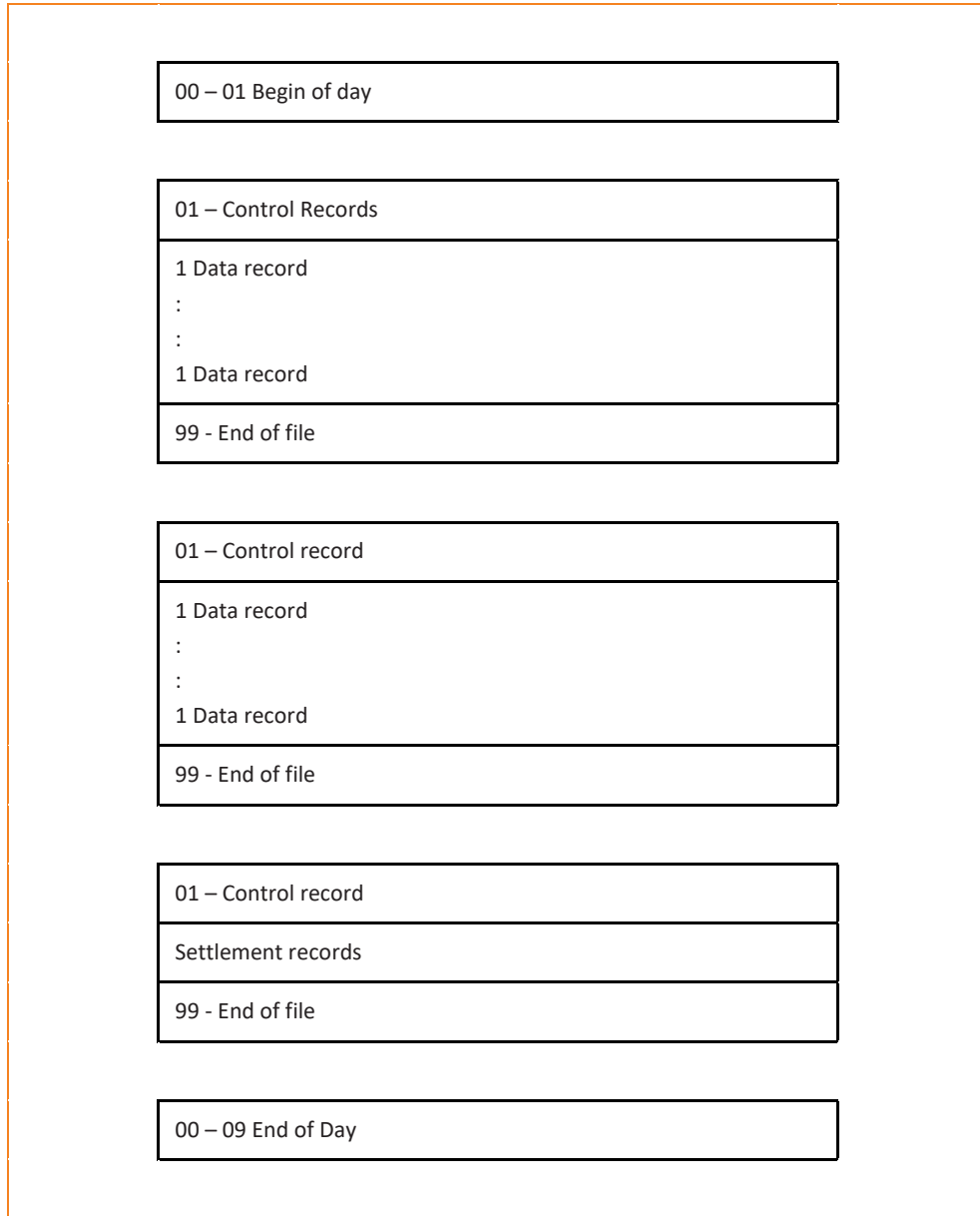
**NOTE:** Each AXS product has a product manual which will contain interface or system specifications, refer to paragraph 2.1.1, of this manual.



*Figure 2: Example of an inward transmission to BankservAfrica*

**NOTE:** Refer to relevant manuals for output specifications.

The figure below depicts an example of an Outward transmission with settlement from BankservAfrica.



*Figure 3: Example of an outward transmission with settlement from BankservAfrica*



### 3. FILE NAMING CONVENTION FOR 8 CHARACTER FILENAMES

#### 3.1. REQUIREMENTS

All files transferred via the AXS delivery platform specified with an eight-character filename must conform to the following format:

**XYZZnnnC**

**X = Application Identifier (A-Z)**

**Y = Sub Application and Direction Identifier (A-Z + 0-9) - defined as XY below**

**ZZ = Bank / Streamcode Combination**

**nnn = File numbering (001 – 999, A00 – Y99)**

**C = File Type**

Table 3: Application Identifiers

X = Application Identifier			
A	AUTC	N	ICMS (CASH)
B	AVS	O	
C	CARD	P	
D		Q	
E	EFT	R	RTC
F		S	SETT
G		T	
H	HCRD	U	UPI
I		V	
J		W	SASW
K	SASA	X	
L		Y	
M	NREG	Z	



**XY = Sub Application Identifier (Per Application Identifier)**

*Table 4: AVS Sub Application Identifier*

AVS					
	SUBSERVICE	DIRECTION		SUBSERVICE	DIRECTION
BA	TO VERIFY	IN	BN		
BB	TO VERIFY	OUT	BO		
BC			BP		
BD	STO VERIFY	IN	BQ		
BE	SVERIFIED	OUT	BR		
BF	VERIFIED	IN	BS		
BG	VERIFIED	OUT	BT	VERIFYVET	OUT
BH	REPORTS	OUT	BU		
BI			BV		
BJ			BW		
BK			BX		
BL			BY		
BM			BZ		

*Table 5: DMCS Sub Application Identifier*

DMCS					
	SUBSERVICE	DIRECTION		SUBSERVICE	DIRECTION
CA	AMEX	IN	CN		
CB	DEBITCRD	IN	CO		
CC	MCI	IN	CP		
CD	MCI	OUT	CQ		
CE			CR	REPORTS	OUT
CF			CS		
CG			CT		
CH	DINERVAL	OUT	CU		
CI	CIS	OUT	CV	VISA	IN
CJ			CW	VISA	OUT
CK	DINERS	IN	CX	VISAVAL	OUT
CL	FLEETCARD	IN	CY	MCIVAL	OUT
CM	AMEXVAL	OUT	CZ		
C0	VISA CARD*	IN	C5	AMEX	OUT
C1	MASTERCARD*	IN	C6	FLEETCARD	OUT
C2	FLEETVAL	OUT	C7	DINERS	OUT
C3			C8		
C4			C9	CSVREP	OUT



\*For internal use only

Table 6: EFT Sub Application Identifiers

EFT					
	SUBSERVICE	DIRECTION		SUBSERVICE	DIRECTION
EA			EN	ONE DAY	IN
EB	EM SAMEDAY	OUT	EO	ONE DAY	OUT
EC	SECREQUEST	IN	EP	ONLREP	OUT
ED	SECREQUEST	OUT	EQ		
EE	EM ONE DAY		ER	REPORTS	OUT
EF	EFTREP	OUT	ES	SAMEDAY	IN
EG	UNPAIDS	OUT	ET		
EH	RECALLS	OUT	EU		
EI			EV	SAMEDAY	OUT
EJ	DATED	IN	EW	CMAFATF	IN
EK	DATED	OUT	EX	RECALLS	IN
EL	SECRESPONS	IN	EY	CMAFATF	OUT
EM	SECRESPONS	OUT	EZ	SARS EFT	OUT

Table 7: NREG Sub Application Identifiers

NREG					
	SUBSERVICE	DIRECTION		SUBSERVICE	DIRECTION
MA			MN		
MB			MO		
MC			MP	NOMADREP	IN
MD			MQ		
ME			MR	NOMADRECON	IN
MF			MS		
MG			MT		
MH			MU		
MI			MV		
MJ			MW		
MK			MX		
ML			MY		
MM			MZ		

Table 8: ICMS Sub Application Identifiers

ICMS					
	SUBSERVICE	DIRECTION		SUBSERVICE	DIRECTION
NA	SREPORTS	OUT	NN	SORDERRESP	OUT





NB	SORTSABI	IN	NO	ORDERS	IN
NC	SORTSABO	OUT	NP	ORDERS	OUT
ND	MSTDATAMNG	OUT	NQ	SORDERRESP	IN
NE			NR	RECONREC	OUT
NF			NS	SORDERREQ	IN
NG	SETTLECON	OUT	NT	SORDERREQ	OUT
NH	REPORTS	OUT	NU	MISDATA	OUT
NI	SORTINGDF	OUT	NV	VAULT	IN
NJ			NW	SORTING	IN
NK	VETREPORTS	OUT	NX	SORTING	OUT
NL			NY	SETTLE	IN
NM			NZ	RECONPAY	OUT
N0			N5		
N1	SORTPAY	OUT	N6		
N2			N7		
N3			N8		
N4			N9		

Table 9: RTC Sub Application Identifiers

RTC					
	SUBSERVICE	DIRECTION		SUBSERVICE	DIRECTION
RA			RN		
RB			RO		
RC			RP		
RD			RQ		
RE			RR		
RF			RS		
RG			RT		
RH			RU		
RI			RV		
RJ			RW		
RK			RX		
RL			RY	BATCH	OUT
RM			RZ	REPORTS	OUT

Table 10: SASW Sub Application Identifiers



SASW					
	SUBSERVICE	DIRECTION		SUBSERVICE	DIRECTION
WA			WN		
WB	BINUPDATE	OUT	WO		
WC	DEDIT CARD	OUT	WP		
WD	BINUPDCSV	OUT	WQ		
WE	REPORTS	OUT	WR		
WF			WS		
WG			WT		
WH			WU		
WI			WV		
WJ			WW		
WK			WX		
WL			WY		
WM			WZ		

Table 11: Settlement Report Sub Application Identifiers

SETTLEMENT REPORTS					
	SUBSERVICE	DIRECTION		SUBSERVICE	DIRECTION
SA	DCARREPS	OUT	SN	CASHREPS	OUT
SB			SO	RPPREPS	OUT
SC	CARDREPS	OUT	SP		
SD			SQ		
SE	EFTREPS	OUT	SR	RTCREPS	OUT
SF	SWIFTREPS	OUT	SS		
SG			ST	AUTHREPS	OUT
SH			SU		
SI			SV	VISAREPS	OUT
SJ			SW	SASWREPS	OUT
SK			SX		
SL			SY		
SM			SZ		

Table 12: Card Listing Sub Application Identifiers

CARD LISTING					
	SUBSERVICE	DIRECTION		SUBSERVICE	DIRECTION
HF	ISSFULL	IN	HT	ACQFULL	OUT
HR	ISSUPDATE	IN	HU	ACQUPDATE	OUT

**ZZ = Bank / Streamcode Combination**

AO.....Z0,  
 AA.....AZ,  
 BA.....BZ, ETC

These are assigned to each participant by BankservAfrica when the participant registers as a live user of the system.

**nnn = File numbering (001 – 999, A00 – YY9)**

Table 13: File numbering

001	through	999
A00	through	A99
B00	through	B99
C00	through	C99
D00	through	D99
E00	through	E99
F00	through	F99
G00	through	G99
H00	through	H99
I00	through	I99
J00	through	J99
K00	through	K99
L00	through	L99
M00	through	M99
N00	through	N99
O00	through	O99
P00	through	P99
Q00	through	Q99
R00	through	R99
S00	through	S99
T00	through	T99
U00	through	U99
V00	through	V99
W00	through	W99
X00	through	X99
Y00	through	Y99



Reserved Sequence Numbers are the following:

- 0Z1 - Begin-of-day;
- 0Z9 - End-of-Day; and
- OSS - Settlement file.

Table 14: File types

C = File Type			
A	Reserved for ACK	N	Reserved for NACK
B		O	
C	Control File	P	
D	Data File	Q	
E		R	
F		S	
G		T	
H		U	
I		V	
J		W	
K		X	
L		Y	
M		Z	

## 4. FILE FORMAT FOR 8 CHARACTER FILENAMES

### 4.1. 01 CONTROL RECORD

Table 15: Control record

Field No.	Field Name	Length	Relative Position	Char-position	Alpha Or Numeric	Field Contents
1	Record Identifier	2	0	1-2	N	Will contain value 01
2	Processing Date	8	+2	3-10	N	Date for which service is running. Format "YYYYMMDD"
3	Service Type	4	+10	11-14	AN	Must be left justified. If the mnemonic is shorter than 4 characters, it must be filled with spaces.
4	Sub-service Type	10	+14	15-24	AN	Must be left justified. If the sub service mnemonic is shorter than 10 characters, it must be filled with spaces.
5	Destination	4	+24	25-28	N	Will contain the designated destination Bank Code.
6	Originator	4	+28	29-32	AN	Abbreviation indicating file originator "ACBJ".
7	File Name	8	+32	33-40	AN	File Naming Convention Refer to paragraph above.
8	File Number	4	+40	41-44	AN	Starts at 1 and is incremented by 1 for every file produced for a specific member for the given service and sub service. There is no relation between the file name and the file number.
9	Data Type	4	+44	45-48	AN	This refers to the type of information held in this file. Data files must have the term "DATA", master files must have "MAST" inserted in this field. The settlement file is identified by the term "SETL" in this field.
10	Data Direction	3	+48	49-51	AN	Will contain the value "IN" to indicate files inward to BankservAfrica Or "OUT", to indicate data out of BankservAfrica
11	Settlement Date	8	+51	52-59	N	Date format "YYYYMMDD"
12	Test-Live Indicator	4	+59	60-63	AN	Value "TEST" for test data Or "LIVE" for production data
13	Record Size	4	+63	64-67	N	Will contain the number indicating the length of each record in the file.
14	Bank Code	4	+67	68-71	N	Will contain the designated destination Bank Code.
15	Report Type	10	+71	72-81	AN	Name of the report when the sub service is for reports. Else spaces.
16	File Type	10	+81	82-92	AN	Name of the file format. This field will contain "XML" for the XML format files. Else spaces.
17	Settlement Window	2	+92	93-94	N	Will contain the Settlement Window number.
18	Transaction Type	30	+94	95-124	AN	Will contain the transaction type for XML files. Will only be used when File Type = 'XML' to uniquely identify the file/transaction type.
19	Filler	nn	+124	125-???	AN	For BankservAfrica use. This area varies according to the different services and their requirements

## 4.2. DATA RECORDS

See relevant manuals for specific service specification documentation.

## 4.3. 99 END OF FILE RECORD

Table 16: End of file Record

Field No.	Field Name	Length	Relative Position	Char-position	Alpha Or Numeric	Field Contents
1	Record Identifier	2	0	1-2	N	Will contain value 99.
2	Processing Date	8	+2	3-10	N	Date for which service is running. Format "YYYYMMDD"
3	Service Type	4	+10	11-14	AN	Must be left justified. If the mnemonic is shorter than 4 characters it must be filled with spaces.
4	Sub-service Type	10	+14	15-24	AN	Must be left justified. If the sub service mnemonic is shorter than 10 characters it must be filled with spaces.
5	Destination	4	+24	25-28	N	Will contain the designated destination Bank Code.
6	Number of Records	6	+28	29-34	N	Indicates the total number of records on this file (includes 01 and 99). Use least significant six digits if count is greater than 999999.
7	Source Identifier	8	+34	35-42	N	This field will contain the 4-digit source identifier or zeroes. This is right justified and will be left padded with zeros.
8	Encrypted Working Key 16	16	+42	43-58	AN	This is a random 16 bit key encrypted under the sender's Zone Control Master Key, see chapter 6
9	MAC of Hash Total	16	+58	59-74	AN	This is a Message Authentication Code, generated using the working key and the HASH TOTAL, see chapter 6. The Message Authentication Code is 8 characters long and will be stored in the 16 character field, padded to the left with zeroes (right justified, zero filled).
10	Hash Total	12	+74	75-86	N	This is a hash total of an agreed set of numeric fields. The calculation of the hash total will differ from one service to another. Refer to the relevant service manuals for the details. The least significant 12 digits should be used.
11	Encrypted Working Key 32	32	+86	87-118	AN	This is a random 32 bit key encrypted under the sender's Zone Control Master Key, see chapter 6
12	Filler	nn	???	???	AN	For BankservAfrica Use Only

#### 4.4. TRANSMISSION CONTROL FILE – START OF DAY

The Transmission File always contains: One control record (00) containing various transaction types.

Table 17: Start of day file

Field No.	Field Name	Length	Relative Position	Char-position	Alpha Or Numeric	Field Contents
1	Record Identifier	2	0	1-2	N	Must contain value 00
2	Transaction Type	2	+2	3-4	N	Must contain value 01
3	Processing Date	8	+4	5-12	N	Date for which service is running. Format 'YYYYMMDD'
4	Service Type	4	+12	13-16	AN	Must be left justified. If the mnemonic is shorter than 4 characters it must be filled with spaces.
5	Sub-service Type	10	+16	17-26	AN	Must be left justified. If the sub service mnemonic is shorter than 10 characters it must be filled with spaces.
6	Destination	4	+26	27-30	N	Will contain the designated destination Bank Code.
7	Originator	4	+30	31-34	AN	Abbreviation indicating file originator "ACBJ".
8	Data Direction	3	+34	35-37	AN	Will contain the value "IN" to indicate files inward to BankservAfrica Or "OUT", to indicate data out of BankservAfrica
9	Test-Live Indicator	4	+37	38-41	AN	Value "TEST" for test data Or "LIVE" for production data
10	Filler	139	+41	42-180	AN	For BankservAfrica use.

## 4.5. TRANSMISSION CONTROL FILE – END OF DAY

Table 18: End of day file

Field No.	Field Name	Length	Relative Position	Char-position	Alpha Or Numeric	Field Contents
1	Record Identifier	2	0	1-2	N	Will contain value 00
2	Transaction Type	2	+2	3-4	N	Will contain value 09
3	Processing Date	8	+4	5-12	N	Date for which service is running. Format 'YYYYMMDD'
4	Service Type	4	+12	13-16	AN	Must be left justified. If the mnemonic is shorter than 4 characters it must be filled with spaces.
5	Sub-service Type	10	+16	17-26	AN	Must be left justified. If the sub service mnemonic is shorter than 10 characters it must be filled with spaces.
6	Destination	4	+26	27-30	N	Will contain the designated destination Bank Code.
7	Originator	4	+30	31-34	AN	Abbreviation indicating file originator "ACBJ".
8	Data Direction	3	+34	35-37	AN	Will contain the value "IN" to indicate files inward to BankservAfrica Or "OUT", to indicate data out of BankservAfrica
9	Test-Live Indicator	4	+37	38-41	AN	Value "TEST" for test data Or "LIVE" for production data
10	Filler	1	+41	42-42	AN	Will contain space.
11	Number of Files	4	+42	43-46	N	Total number of files for the day for the service and sub service – (excluding transmission control files).
12	Number of Records	8	+46	47-54	N	Total number of records in the data files for the day (includes control (01) and end of file (99) records, excludes all transmission control files).
13	Filler	126	+54	55-180	AN	For BankservAfrica use.



## 4.6. TRANSMISSION CONTROL FILE – ACK/ NACK FILE

Table 19: ACK/ NACK File

Field No.	Field Name	Length	Relative Position	Char-position	Alpha Or Numeric	Field Contents
1	Record Identifier	2	0	1-2	N	Will contain value 00
2	Transaction Type	2	+2	3-4	N	This field could contain one of the following: - SENDER ➤ "01" - Beginning of day ➤ "09" - End of day RECEIVER ➤ "51" - Beginning of day (ACK) ➤ "61" - Beginning of day (NACK) ➤ "52" - File (ACK) ➤ "62" - File (NACK) ➤ "59" - End of day (ACK) ➤ "69" - End of day (NACK)
3	Processing Date	8	+4	5-12	N	Date for which service is running. Format 'YYYYMMDD'
4	Service Type	4	+12	13-16	AN	Must be left justified. If the mnemonic is shorter than 4 characters it must be filled with spaces.
5	Sub-service Type	10	+16	17-26	AN	Must be left justified. If the sub service mnemonic is shorter than 10 characters it must be filled with spaces.
6	Destination	4	+26	27-30	N	Will contain the designated destination Bank Code.
7	Originator	4	+30	31-34	AN	Abbreviation indicating file originator "ACBJ".
8	Data Direction	3	+34	35-37	AN	Will contain the value "IN" to indicate files inward to BankservAfrica Or "OUT", to indicate data out of BankservAfrica
9	Test-Live Indicator	4	+37	38-41	AN	Value "TEST" for test data Or "LIVE" for production data
10	File Name	8	+41	42-49	AN	File Naming Convention Refer to paragraph above.
11	File Number	4	+49	50-53	N	Starts at 1 and is incremented by 1 for every file produced for a specific member for the given service and sub service. There is no relation between the file name and the file number.
12	Error Code occurs 10	2	+53	54-55	AN	Refer below.
13	Filler	125	+56	56-180	AN	For BankservAfrica use.



#### 4.6.1. ERROR CODES

Error Code and description to explain the reason for the rejection of a file.

Table 20: Control record error codes

Error Code	Description
01	Invalid record identifier
02	Invalid processing date
03	Invalid service/subservice
04	Invalid member
05	Invalid BankservAfrica center
06	Invalid Filename/number
07	Invalid Date Type
08	Invalid Data Direction
09	Invalid Transaction Type
10	Invalid Window/Time for this service
11	Invalid internal/external filename
12	No begin of Day File
13	Begin of Day file not acked
16	Data File already acked

Table 21: End of file record error codes

Error	Description
21	Invalid record identifier
22	Invalid number of records
23	Invalid Hash Value
24	Number of records exceed maximum
25	Invalid authentication



*Table 22: End of day file error codes*

Error	Description
41	Invalid record identifier
42	Invalid number of files
43	Invalid number of records

*Table 23: Physical file error codes*

Error	Description
91	Invalid File Name
92	File does not exist
93	Invalid File Type
94	User not live for service
99	AXS timeout – retries exhausted



## 5. OVERVIEW OF XML (ISO20022) TRANSMISSION SYSTEM

### 5.1. XML INPUT

The Automated Transmission Service, (AXS) enables participants using XML to connect directly to the central processing centre for electronic submission and receipt of financial and non-financial data.

Data is to be submitted electronically in the format specified in Chapters 4 & 5 – XML Application Interface. A reply file will be returned to the participant on successful transmission. The reply file can be either an acknowledgment indicating that the file has been accepted for further validation, or it could be a negative acknowledgement indicating that the file has been rejected.

### 5.2. XML FUNCTIONAL OVERVIEW

#### 5.2.1. XML INWARD TRANSMISSION INTO THE BATCH SWITCH INCLUDES:

- A TCP/IP session must be established with the batch switch.
- A file transfer session must be initiated from the participant's transmission platform to batch switch transmission platform.
- Upon receipt of a complete file, the file will be validated according to the validation procedures for the service type. The service is determined from the file's external name. Data integrity and authenticity of the originator will be checked, as well as whether the file was received within the specified time window.
- Should a file fail structure and integrity validation checks, a negative acknowledgement file will be returned to the originating bank.
- If a file passes structure and integrity validation checks, the file will be processed according to the validation procedures for the appropriate service.
- SOT and EOT are sent once per sub-service, per processing day.
- If the EOT is sent in error then BankservAfrica does not require another SOT, BankservAfrica Operations Department must be informed and the EOT will be lifted for that particular sub-service so that the bank can continue processing.
- Only data files must be included in the number of files and number of records count in the EOT file. If a NACK is encountered on the file, then it does not get added to the number of files and number of records. Only data files that were successfully received will be included in the final count.



#### 5.2.2. XML OUTWARD TRANSMISSION FROM THE BATCH SWITCH TO PARTICIPANTS INCLUDES:

- The batch switch transmission platform will establish a TCP / IP session with the participant's transmission platform.
- A file transfer session is then initiated to transfer files, from the batch switch's transmission platform to the destination transmission platform.
- Upon receipt of a complete file from the transmission platform, the file must be validated according to the validation procedures for the appropriate service. The service is determined from the file's name. Data integrity and authenticity of the originator must also be checked.
- Should the file fail validation checks, a negative acknowledgement file must be returned to the batch switch, specifying the reason a particular file was rejected. The received file must be renamed or deleted.
- If a file passes the validation checks, it should be transferred to the destination system for further processing, and a positive acknowledgement file must be returned to BankservAfrica batch mandate switch
- SOT and EOT are sent once per sub-service, per processing day.
- If the EOT is sent in error then BankservAfrica does not require another SOT, BankservAfrica Operations Department must be informed and the EOT will be lifted for that particular sub-service so that the bank can continue processing.
- Only data files must be included in the number of files and number of records count in the EOT file. If a NACK is encountered on the file, then it does not get added to the number of files and number of records. Only data files that were successfully received will be included in the final count.

## 6. APPLICATION INTERFACE FOR XML (ISO20022) FILES

### 6.1. APPLICATION PROTOCOLS

#### 6.1.1. INTRODUCTION

This section specifies application level protocols for transmission between BankservAfrica and participating banks. The purpose of application-level protocols is to authenticate transmitting parties and ensure the integrity of the data.

#### 6.1.2. PROPOSED PROTOCOLS

This specification is based on assumptions that:

- The sender is in control; and
- The sender is responsible for delivery.

#### 6.1.3. CODE SET

The code set comprises of the following:

- Transmission:
  - Input to BankservAfrica: XML; and
  - Output from BankservAfrica: XML.

The flow of data is best described by means of the table below:

Table 24: XML Data flow

Sender	Receiver
Start of Transmission -----> (Check if other party is up and running) Transmission file type = S	<-----Start of transmission Ack (go ahead, I am up and running) Transmission file type = A
	<-----Start of transmission Nack (Error – Start of transmission) Transmission file type = N
Send data file 1 -----> (File containing ISO 20022 message) Transmission file type = D	<-----Receiver Ack file 1 (Receiver pre-validates and accepts) Transmission file type = A
	<-----Receiver Nack file 1 (Receiver pre-validates and rejects) Transmission file type = N
Send data file 2 -----> (File containing ISO 20022 message) Transmission file type = D	<-----Receiver Ack file 2 (Receiver pre-validates and accepts) Transmission file type = A
	<-----Receiver Nack file 2 (Receiver pre-validates and rejects) Transmission file type = N
Send data file 3 -----> (File containing ISO 20022 message)	<-----Receiver Ack file 3 (Receiver pre-validates and accepts)

Transmission file type = D		Transmission file type = A
		<-----Receiver Nack file 3 (Receiver pre-validates and rejects) Transmission file type = N
End of Transmission -----> (Once all files have been acknowledged for the service) Transmission file type = E		<-----End of Transmission Ack (Receiver checks the day's transmission for the specific service) Transmission file type = A
		<-----End of Transmission Nack (Receiver checks the day's transmission for the specific service) Transmission file type = N

#### 6.1.4. VALIDATION

Specific validation procedures are defined for each service type in the respective Interface Specifications.

#### 6.1.5. MESSAGE LAYOUT

Two types of files / messages are used in transmission sessions: transmission control messages and data files.

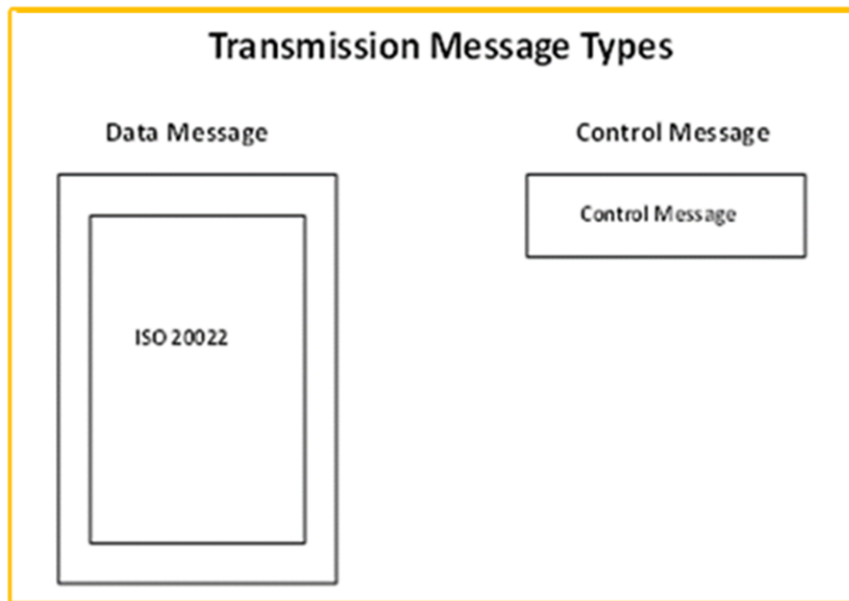


Figure 4: Transmission message types

- Control messages are simple message with few elements. These messages are used to indicate
  - Start of transmission (last character in file name is a **S**)
  - File acknowledgement (last character in file name is a **A**)
  - Negative acknowledgement (last character in file name is a **N**)
  - End of transmission (last character in file name is a **E**)
- Data files contain ISO 20022 messages.

## 6.2. EXAMPLE OF SERVICES

Transmission services comprise inward and outward services. Figure 2 is an example of inward transmission to the batch switch.

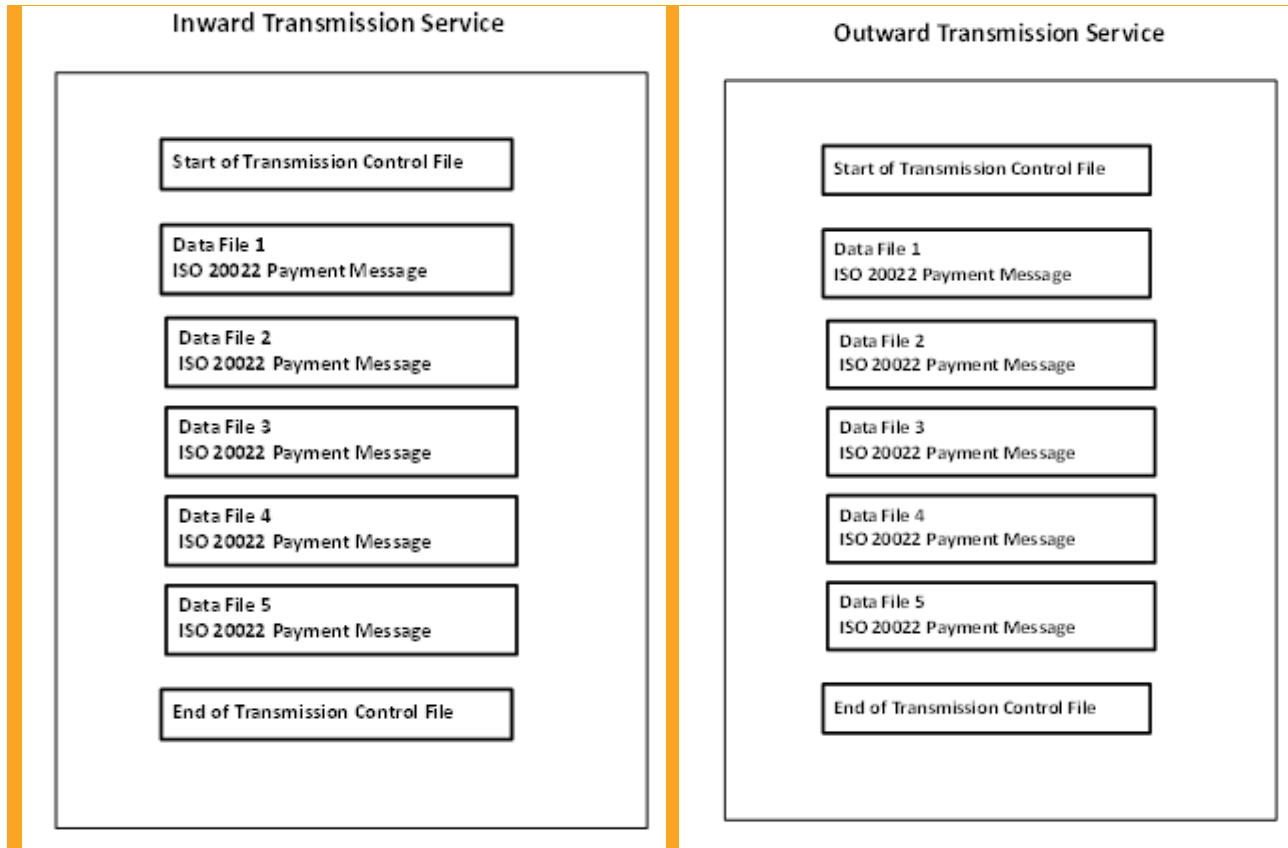


Figure 5: Example of inward transmission to BankservAfrica

Figure 6: Outward transmission service from BankservAfrica

### START OF TRANSMISSION MESSAGES

- The “start of transmission” message must have a file number of zero, and a last character in the file name must be equal to “S”.
- Start of transmission messages are control messages.
- This message indicates the opening of a transmission session for the service subservice combination.
- The message reference element in the control message must contain “SOT”.

### DATA FILES

- Data files contain ISO 20022 messages.
- Data files are identified by the last character in the file name having the value of “D”.





## CONTROL MESSAGES

- Start of day, Ack (acknowledgement) and Nack (negative acknowledgement) messages are control messages.
- When a message is received intact, an acknowledgement message must be returned containing the same file name with the last character in the file name changed to an “A”.
- Similarly, when a message is corrupt or fails structure validation on receipt, a negative acknowledgement message must be returned having the last character in the file name changed to an “N”.

## END OF TRANSMISSION MESSAGES

End of transmission messages must have the last character in the file name equal to “E” and contain “EOT” in a message reference field. This file contains the following controls:

- Number of files sent; and
- Number of records sent.

Ack and Nack messages are used to confirm or reject start of transmission, data and end of transmission messages and are used in all file transmission mechanisms (even those that have their own in-built confirmation messaging).

## 6.3. XML TRANSMISSION FILE SIZES

### Bulk file transfer mechanisms

The maximum number of records per file using dedicated lines or other high speed transmission mechanisms is determined the service and or line speeds.

## 6.4. XML SUBSERVICES FOR AUTHENTICATED COLLECTIONS

Table 25: XML Subservices for Authenticated Collections

Sub service	Direction	Type	Sub service	Direction	Type
DRINP	IN	Collections	MANAM	IN	Mandates
RTINP	IN	Collections	MANAC	IN	Mandates
SPINP	IN	Collections	MANRT	IN	Mandates
SRINP	IN	Collections	ST101	IN	Mandates
RIINP	IN	Collections	MANCN	IN	Mandates
DDINP	IN	Collections	MANIN	IN	Mandates
CLINP	IN	Collections	MANRI	IN	Mandates
RIOUT	OUT	Collections	BEINP	IN	Collections
RTOUT	OUT	Collections	REINP	IN	Collections
ST009	OUT	Collections	RBINP	IN	Collections
SPOUT	OUT	Mandates	MANCO	OUT	Mandates
ST007	OUT	Mandates	ST105	OUT	Mandates
ST008	OUT	Mandates	ST104	OUT	Mandates
ST003	OUT	Collections	ST103	OUT	Mandates
ST004	OUT	Collections	ST102	OUT	Mandates
ST006	OUT	Collections	ST100	OUT	Mandates
ST002	OUT	Collections	ST011	OUT	Mandates
ACSET	OUT	Collections	ST010	OUT	Mandates
SROUT	OUT	Mandates	MANRF	OUT	Mandates
CLOUT	OUT	Collections	MANOT	OUT	Mandates
DDOUT	OUT	Collections	MANOM	OUT	Mandates
DROUT	OUT	Collections	MANOC	OUT	Mandates
ST901	OUT	Collections	MANRO	OUT	Mandates
ST902	OUT	Collections	ST106	OUT	Mandates
BEOUT	OUT	Collections	RBOUT	OUT	Collections
REOUT	OUT	Collections	ST903	OUT	Collections

## 7. AXS SECURITY PROCESS FOR EIGHT CHARACTER FILENAMES

### 7.1. PLAYERS IN THE AUTHENTICATION PROCESS

The authentication process described below details actions required of the sender of the data, also referred to as the *source*, and the *receiver* of the data. In the AXS file transfer session, BankservAfrica will either act as a source or a receiver of data, depending on whether file transfers are to participants or from participants. All players initiating a file transfer will have a *source identifier*. The source identifier for Banks is the Bank member number. The source identifier allocated to BankservAfrica is 9999.

### 7.2. TECHNIQUE

The authentication process uses a transaction key scheme where an encrypted working key (TAK) is used to obtain a Message Authentication Code (MAC) of specified field. This technique requires working keys to be generated for every transmission file sent.

### 7.3. EXCHANGE OF KEYS

Transmitting partners are expected to load component keys at a location specified by BankservAfrica. Players are to use Zone Master Keys to generate encrypted working keys that are to be sent with transmission files. Players are expected to update Zone Master Keys periodically in keeping with prudent audit requirements.

### 7.4. PROCESS

#### 7.4.1. THE PARTICULARS OF THE PROCESS

AXS Security Process authenticates the source through the Zone Master Key (ZMK), Encrypted Working Key, MAC of Hash and Hash Total. The process uses an encrypted working key to obtain/validate a Message Authentication Code (MAC). In this phase the hash total of an agreed set of numeric fields is used in the generation/validation of the MAC. The calculation of the hash total is specific to the service and may differ from one service to the next.

#### 7.4.2. ACTIONS REQUIRED OF THE SENDER OF A TRANSMISSION FILE

When transmitting a file, the following fields must be supplied as detailed in the end-of-file record (record id 99) contained in paragraph 3.2.3:

- SOURCE-ID - 8 BYTES
- ENCRYPTED-WORKING-KEY - 16 or 32 BYTES
- MAC-OF-HASH TOTAL - 16 BYTES
- HASH-TOTAL - 12 BYTES



The following steps must be used by the sender to obtain MAC of the hash total:

1. Obtain a 12 digit hash total for the specified service
2. Generate a random working key under the sender's LMK.
  - 2.1 Length of key will be 16 bytes for single or 32 bytes for double length authentication.
3. Use the working key to obtain a MAC of the hash total.
  - 3.1. In the event that a 12 digit hash is incompatible with your HSM when using double length keys, the hash total can be padded to the left with 4 fixed ascii characters, 0000 (four zeroes), when generating the MAC. The extra 4 characters must then be discarded from the hash when writing to the 99 record.
4. Translate the working key from LMK (local key) to ZMK (exchanged key) encryption.
5. Insert the source identifier, the encrypted working key, the hash total and the MAC of the hash total in the end-of-file record.

#### 7.4.3. ENCRYPTION ROUTINE

The encryption routine used is the ANSI X9.9 standard 64 bit DES encryption algorithm. The 4-digit source identifier will be stored in an 8-byte field padded to the left with zeroes (right justified zero filled). Likewise the 8-digit calculated MAC of the source identifier will be stored in the 16-byte field padded to the left with zeroes (right justified zero filled). The hash total will be the 12 least significant digits of a hash calculated for that service.

#### 7.4.4. ACTIONS PERFORMED BY THE RECEIVER OF A TRANSMISSION FILE

The following actions are performed by a receiver to complete the authentication process:

1. The source identifier is used to obtain the ZMK of the sender.
2. The working key is translated from under the source's ZMK to a key encrypted under the receiver's LMK.
3. The working key, encrypted under the LMK, will be used to verify the MAC of the hash total.

### 7.5. SECURITY PROCESS FOR XML (ISO20022) FILES

#### 7.5.1. PROCESS OF AUTHENTICATING MESSAGES

To validate the source of the sensitive information between banks and BankservAfrica, transmitting parties use an algorithm to generate and verify Message Authentication Codes appended to messages.

To facilitate this process, transmitting parties are expected to exchange Zone Control Master keys (ZMK) with BankservAfrica (Public Key Infrastructure).

The authentication process uses a transaction key scheme where an encrypted **working key** (TAK) is used to obtain a Message Authentication Code (MAC) of specified field. This technique requires **working keys** to be generated for every transmission file sent.



## 7.5.2. ACTIONS REQUIRED OF THE SENDER OF A TRANSMISSION MESSAGE

### PROCESS FOR AUTHENTICATED COLLECTIONS

When transmitting a message, the following algorithm must be used to generate and include a message authentication code (MAC).

1. For pacs.003 messages, obtain the sum of the debtor account numbers and amounts in the message. For pacs.004 messages, sum the amounts in the message. The amounts must be in cents (i.e. ignore the decimal point). Truncate the sum to the least significant 18 digits.
2. Populate the **<CtrlSum>** in Group Headers of messages with the total of the sum obtained above.
3. Generate a random **working key** of 16 digits under the sender's Local Master Key (**LMK**).
4. Generate a **MAC** (8 digits) using the working key and the total sum obtained above using ANSI X9.9 MAC process.
5. Encrypt the working key from the sender's **LMK** using the Zone Control Maser Key **ZMK** key (exchanged key).
6. Insert the encrypted **working key** (16 digits) and the **MAC** (8 digit MAC) into **<Authstn><Prtry>** element (24 digits).

## 7.5.3. ACTIONS PERFORMED BY THE RECEIVER OF A TRANSMISSION MESSAGE

### PROCESS FOR AUTHENTICATED COLLECTIONS

The following actions are performed by a receiver to complete authentication of a received message:

1. From the Message identifier, obtain the originator of the message. Use this to obtain the sender's Zone Control Master key (ZMK).
2. Extract the encrypted **working key** from the **<CtrlSum>** and decrypt the working key using the sender's ZMK.
3. For pacs.003 messages, obtain the sum of the debtor account numbers and amounts in the message. For pacs.004 messages, sum the amounts in the message. The amounts must be in cents (i.e. ignore the decimal point). Truncate the sum to the least significant 18 digits.
4. Verify the MAC in the messages to a **MAC** (8 digits) generated using the decrypted **working key** and the total sum obtained above using ANSI X9.9 MAC process.

#### 7.5.4. EXAMPLE OF GENERATING A MAC FOR AC MESSAGES

##### STEP 1

Add account numbers with their associated amounts, taken in cents, and place this sum accumulator field.

Account Numbers	Amounts	Accumulator
1234567890123456789	12.34	1234567890123458023
1234567890123456	123.45	1234567890135801
1234567890123456789	12345678901.23	1234569124691346912

##### STEP 2

Add all accumulated amounts together and place the sum in the Control Sum <CtrlSum>.

Accumulator
1234567890123458023
1234567890135801
<u>1234569124691346912</u>
2470371582704940736

Separate the least significant 18 digits for later use in an ANSI X9.9 MAC process.

**470371582704940736**

##### STEP 3

Generate a Single Length DES TAK key (random working key) under your local TMK (Terminal Master Key)

Call Host Security Module with test key (eg: 2323232323232323).

##### STEP 4

Encrypt the working key from the sender's LMK using the exchanged ZMK.

##### STEP 5

Generate a MAC (triple DES encryption) of the least significant 18 digits **2470171582704940736**, using the random key 2323232323232323

Resultant MAC = 0000000AA556E65

Select the 8 least significant digits = AA556E65

##### STEP 6

Insert the encrypted working key from step 4 (16-digits) and the encrypted hash total MAC (8-digits) into the Message Authentication Code <Authstn><Prtry> in the pacs.003 or pacs.004 message.

<Authstn>						
<Prtry>	Message Authentication Code:	Text	128	M	24AN	The first 16 digits will contain the encrypted working key and the last 8 digits of the MAC of the hash total of destination account numbers and amounts,
</Prtry>						
</Authstn>						



## 8. COMPRESSION METHODS

### 8.1. FILE COMPRESSION

BankservAfrica will support the following methods for file compression and decompression.

- Zip; and
- Gzip.

### 8.2. APPLICATION PROTOCOL COMPRESSION

**Connect Direct:** caters for application protocol compression.

**XCOM:** CATERS FOR APPLICATION PROTOCOL COMPRESSION.

## 9. FILE TRANSFER PROTOCOLS

- XCOM
- CONNECT DIRECT
- SFTP
- SCP
- WEB-SERVICES
- NETSERVICES (BACKUP)