Electronic Submission of Data from Pay & Account Offices (e-PPO)

Bank Interface

Electronic submission of PPO data from Pay & Account offices to Central Pension Accounting Office and finally to CPPCs of Banks.

NIC-Central Pension Accounting Office
25/01/2018

1st Revised on 28/07/2020

2nd Revised on 24/09/2020

Introduction:

System of electronic processing of PPO Booklet is being developed under PFMS. Once this system is implemented, PPO booklet which is currently prepared in handwriting will be replaced with electronic file(pdf). After this there will be no movement of paper documents. CPAO will get the electronic PPO(henceforth called as ePPO) from PFMS along with data in XML format. Both the data and ePPO will be digitally signed by the concerned Pay & Account Officer.

XML data of ePPO will be incorporated in the PARAS database of CPAO. After thorough scrutiny of data and ePPO, CPAO will issue Special Seal Authority for bank in electronic format. eSSA along with data again in XML format will be send to bank in their SFTP directory, for further consumption and action by CPPC.

Objectives to be achieved:

- Streamline the movement of Pension Payment Orders between PAO to CPAO and then to BANK.
- To eliminate errors in data by eliminating data entry at CPAO and Banks.
- Fast and efficient data processing at CPAO and Banks.
- To create an efficient but secured Paperless-processing Application.
- To capture Photo of Pensioner, Spouse, Signature of Pensioner and spouse and biometric information.
- To create an efficient, secure, cost effective communication, integration between systems at CPAO, PAO and Banks.
- To utilize existing IT Infrastructure to provide a cost effective solution.
- To update database at bank end using ePPO data and to have synchronized data at PAO, CPAO and Banks.

Issues Involved:

- To allot digital signature to all PAOs who are authorized to sign PPO booklet.
- To upgrade IT infrastructure at PAO level.
- Checking of authenticity of PPO Number received electronically.
- To avoid fake PPO number generation.
- To maintain directory of PAO authorized to sign PPO and update this directory on real time basis.
- To devise computer printable format of PPO in place of PPO booklet.
- Creation of central portal for providing web interface to PAOs, Banks and Pensioners.
- Banks to create sftp sites at CPPC level wherein CPAO will push the ePPOs.

- To maintain directory of CPAO officers authorized to sign SSA and update it on real time basis.

Proposed System:

In brief:
PAO will keep on processing the pensions as he is presently doing. PAO will utilize Pension Module under PFMS to process the pension case. This module is linked with BHAVISHYA s/w of DPPW. Data entered by Head of Office under BHAVISHYA will be visible to PAO under PFMS to process the case. PAO will scrutinize the data thoroughly after comparing with the paper documents he receives from HOO. Once satisfied he will finalize the data and will create the PPO booklet as ePPO file and digitally signs it. He will freeze the data by digitally signing it with his digital signatures. CPAO will pull the ePPO data into PARAS dabatase for further processing.

Since digitally signed data is now available with CPAO, it can take action on the PPO data. In case of any discrepancy CPAO can revert back the case/data to PAO, who will be then be allowed to make further changes to the data. If CPAO found the data to be correct then authorized person can freeze the data by putting his/her digital signature. From here nobody will be allowed to change the data.

CPAO will generate the SSA as PDF file which will be digitally signed by the authorized signatory. This PDF file will be send to CPPC of bank, which will further allow the paying branch to view it and print it for handing over to the pensioner as pensioner's copy. CPPC may also print it and keep it for record keeping. Once the system is stabilized the paper movement between PAO, CPAO and Banks will be eliminated.

Process Breakup/Description:

1. **Case generation by HOO**
    a. Pension case will be initiated by Head of Office(HOO) in BHAVISHYA s/w.
    b. HOO will fill up the forms and will upload the photographs of pensioner and family pensioner along with specimen signature of pensioner.
    c. HOO will finalise the case by submitting the case under BHAVISHYA.
2. **Case processing by PAO.**
    a. PAO to receive the paper documents from HOO as being done presently.
    b. Data of case under BHAVISHYA will be reflected in PENSION Module of PFMS.
    c. PAO will view the data under "PENSION MODULE" of PFMS.
    d. Once he is satisfied, he will finalize the case.
    e. PAO will finalise the case by digitally signing the PPO booklet as ePPO along with data in XML format.
    f. PAO will submit the case to PFMS.

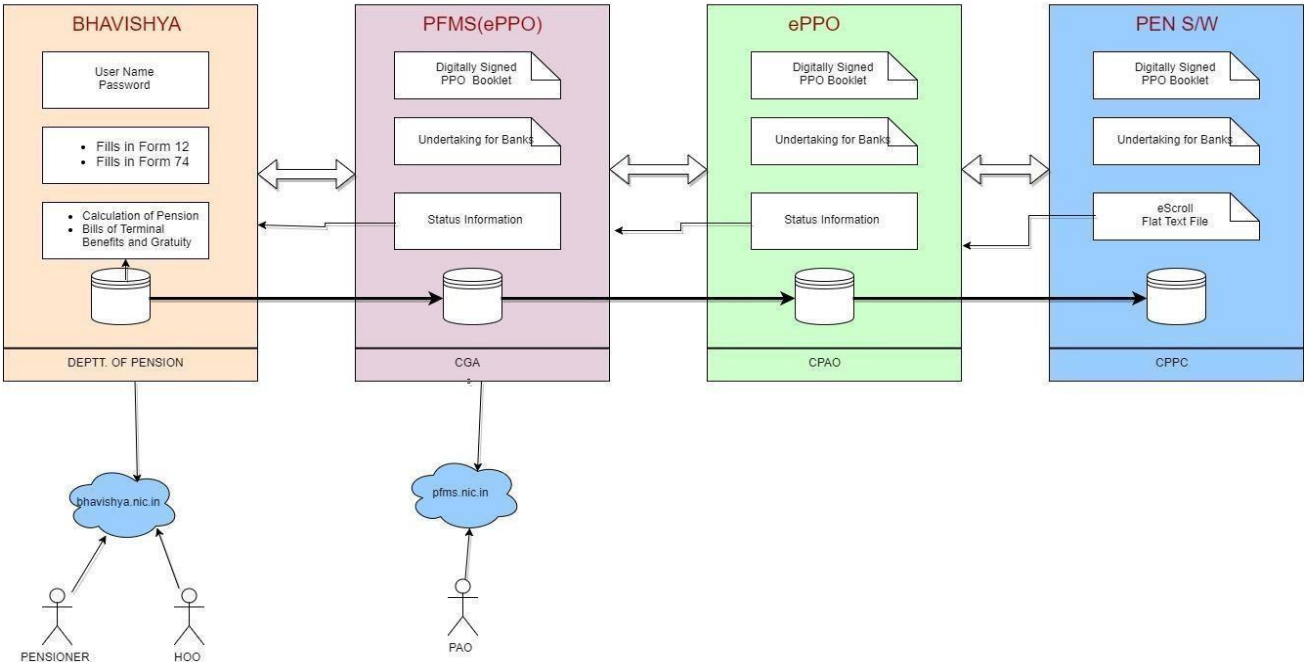
3. **Scrutiny of data by CPAO.**
    a. Data from ePPO site of CPAO will be downloaded and inserted into tables of PARAS database.
    b. When the concerned section will key in the PPO no. for further processing, the downloaded data will be visible to the operator. Here no editing of data will be allowed and in case of any discrepancy of data, the case should be revered back to the PAO.
    c. Section will be aided with automatic tools for making the validation, range and other checks.
    d. Once satisfied, the signing authority will digitally sign the data.
    e. SSA as PDF file will be generated and this also will be digitally signed by the authorized signatory.

4. **Sending ePPO to banks.**
    a. At a scheduled time, all the ePPO pdf files and data in XML format will be extracted from the database and placed in a folder assigned to each and every CPPC.
    b. At a scheduled time, all the files from the ePPO folders will be pushed to sftp site of banks.
    c. The status information about the pushed PPO files will be available on the ePPO website of CPAO.

5. **Processing at CPPCs.**
    a. CPPC will receive the ePPO in their sftp folders.
    b. CPPC will import the ePPO files in their software systems for further processing.
    c. CPPC to make this data available to paying branches for further processing and updating by paying branches.
    d. Paying branch will take a print out of ePPO pdf file and will hand over to pensioner as pensioner copy.

Once implemented, there will be seamless transfer of PPO from PAO to CPAO to Banks as ePPO.

ePPO



Files to be pushed to SFTP of CPPC:

S.No.	Description	File Type	File nomenclature	Example
1	ePPO Booklet	PDF	F<SSA_NO><-8 digit date on which file was generated and sent to bank (YYYYMMDD)>.pdf	F1724884-20180125.pdf
		XML	F<SSA_NO><-8 digit date on which file was generated and sent to bank (YYYYMMDD)>.xml	F1724884-20180125.xml
2	Undertaking	PDF	U<SSA_NO><-8 digit date on which file was generated and sent to bank (YYYYMMDD)>.pdf	U1724884-20180125.pdf
3	eSSA	PDF	N<SSA_NO><-8 digit date on which file was generated and sent to bank (YYYYMMDD)>.pdf	N1724884-20180125.pdf
		XML	N<SSA_NO><-8 digit date on which file was generated and sent to bank (YYYYMMDD)>.xml	N1724884-20180125.xml
4	Instructions	PDF	R<SSA_NO><-8 digit date on which file was generated and sent to bank (YYYYMMDD)>.pdf	R1724884-20180125.pdf

Annexure-I
Format of ePPO
(Electronic Booklet)

SL NO.	XML TAGS	DESCRIPTION	DATATYPE
1	<PPONO>331951700524</PPONO>	PPO(PENSION PAYMENT ORDER) NUMBER	VARCHAR
2	<PPODate>2017-10-23</PPODate>	PPO DATE	DATE
3	<DiaryNumber>W03319517100001</DiaryNumber>	PAO DIARY	VARCHAR
4	<ClassOfPension>A</ClassOfPension>	PENSION CLASS	VARCHAR
5	<PensionHead>2071</PensionHead>	PENSION HEAD	VARCHAR
6	<SubMajorHead>1</SubMajorHead>	SUB-MAJOR HEAD	VARCHAR
7	<MinorHead>101</MinorHead>	MINOR HEAD	VARCHAR
8	<Votedcharged>Voted</Votedcharged>	VOTED/CHARGED	VARCHAR
9	<FileNo>233212\2017\1</FileNo>	PAO PENSION FILE NUMBER	VARCHAR
10	<BankName>CORPORATION BANK</BankName>	BANK NAME	VARCHAR
11	<BankBSRCode>0350385</BankBSRCode>	BANK BSR CODE	VARCHAR
12	<BankAddress>NEW DELHI-LODHI COMPLEX GROUND FLOOR, BLOCK II, CGO COMPLEX PHASE I 110003</BankAddress>	BANK ADDRESS	VARCHAR
13	<Accountno>037100101024892</Accountno>	BANK ACCOUNT NUMBER	NUMBER
14	<PSName>Mr. GANGA PRASAD </PSName>	PENSIONER NAME	VARCHAR
15	<Adhaarno />	AADHAR NUMBER	NUMBER
16	<PAN>ADMPP4337L</PAN>	PAN NUMBER	VARCHAR
17	<Email>ganga.prasad@nic.in</Email>	PENSIONER EMAIL	VARCHAR
18	<MobileNo>9810207415</MobileNo>	PENSIONER MOBILE NUMBER	NUMBER
19	<DDOCode>233212</DDOCode>	DDO CODE(DRAWING AND DISVERSING OFFICER CODE)	VARCHAR
20	<RetiredFrom>DDO, NIC,(Headquarters), DELHI</RetiredFrom>	RETIRED OFFICE FROM	VARCHAR
21	<Group>A</Group>	OFFICER GROUP	VARCHAR
22	<Designation>DEPUTY DIRECTOR</Designation>	DESIGNATION	VARCHAR
23	<PermanentAddress1>Village Tikari, P.O Kanti (Jasra) </PermanentAddress1>	PENSIONER PERMANENT ADDRESS	VARCHAR
24	<PermanentDistrict>ALLAHABAD</PermanentDistrict>	PENSIONER PERMANENT DISTRICT	VARCHAR
25	<PermanentState>UTTAR PRADESH</PermanentState>	PENSIONER PERMANENT STATE	VARCHAR
26	<PermanentPinCode>232307</PermanentPinCode>	PENSIONER PERMANENT PIN CODE	VARCHAR
27	<Naitionality>INDIA</Naitionality>	NATIONALITY	VARCHAR
28	<Gender>M</Gender>	GENDER	VARCHAR
29	<DateOfBirth>1957-10-08</DateOfBirth>	DATE OF BIRTH	DATE
30	<JoiningDate>1981-12-07</JoiningDate>	JOINING DATE	DATE
31	<RetirementDate>2017-10-31</RetirementDate>	RETIREMENT DATE	DATE
32	<DateOfDeath>1900-01-01</DateOfDeath>	DATE OF DEATH	DATE
33	<QS_YEAR>35</QS_YEAR>	QUALIFYING SERVICE YEAR	VARCHAR
34	<QS_MONTH>10</QS_MONTH>	QUALIFYING SERVICE MONTH	VARCHAR
35	<QS_DAY>25</QS_DAY>	QUALIFYING SERVICE DAY	VARCHAR
36	<NQS_YEAR>00</NQS_YEAR>	NON QUALIFYING SERVICE YEAR	VARCHAR

37	<NQS_MONTH>01</NQS_MONTH>	NON QUALIFYING SERVICE MONTH	VARCHAR
38	<NQS_DAY>17</NQS_DAY>	NON QUALIFYING SERVICE DAY	VARCHAR
39	<AQS_YEAR>00</AQS_YEAR>	ADDITIONAL QUALIFYING SERVICE YEAR	VARCHAR
40	<AQS_MONTH>00</AQS_MONTH>	ADDITIONAL QUALIFYING SERVICE MONTH	VARCHAR
41	<AQS_DAY>00</AQS_DAY>	ADDITIONAL QUALIFYING SERVICE DAYS	VARCHAR
42	<TQS_YEAR>35</TQS_YEAR>	TOTAL QUALIFYING SERVICE YEAR	VARCHAR
43	<TQS_MONTH>09</TQS_MONTH>	TOTAL QUALIFYING SERVICE MONTH	VARCHAR
44	<TQS_DAY>08</TQS_DAY>	TOTAL QUALIFYING SERVICE DAY	VARCHAR
45	<TotalQualifyingService>350908</TotalQualifyingService>	TOTAL QUALIFYING SERVICE	DATE
46	<LastPayDrawn>93800</LastPayDrawn>	LAST PAY DRAWN	VARCHAR
47	<PayScale>67700-208700</PayScale>	PAY SCALE	VARCHAR
48	<AvgEmol>93800</AvgEmol>	AVERAGE EMOLUMENTS	VARCHAR
49	<EmolFamilyPension>93800</EmolFamilyPension>	FAMILY PENSION EMOLUMENTS	VARCHAR
50	<EmolRGDG>98490</EmolRGDG>	EMOLUMENTS RETIREMENT GRATUITY CUM DEATH GRATURITY	VARCHAR
51	<ExGratiaPayment>0</ExGratiaPayment>	EX-GRATIA PAYMENT	VARCHAR
52	<NPA>0</NPA>	NON PRACTICING ALLOWANCE	VARCHAR
53	<AnyOtherPay>0</AnyOtherPay>	ANY OTHER PAYMENT	VARCHAR
54	<Level>11</Level>	PAY LEVEL	VARCHAR
55	<Index>12</Index>	PAY INDEX	VARCHAR
56	<GradePay>0</GradePay>	GRADE PAY	VARCHAR
57	<Med_Allow />	MEDICAL ALLOWANCE	VARCHAR
58	<Med_Date>1900-01-01</Med_Date>	MEDICAL ALLOWANCE DATE	DATE
59	<RGDGNotByBank>1625085</RGDGNotByBank>	RETIREMENT GRATUITY /DEATH GRATUITY NOT TO BE PAID BY BANK	VARCHAR
60	<PensionAmount>46900</PensionAmount>	PENSION AMOUNT	NUMBER
61	<DateofCommencement>2017-11-01</DateofCommencement>	DATE OF COMMENCEMENT	DATE
62	<AmountCommuted>18760</AmountCommuted>	COMMUTED AMOUNT	NUMBER
63	<DateOfRestoration>On completion of 15 years of reduced monthly pension after commutation</DateOfRestoration>	DATE OF RESTORATION	DATE
64	<ReducedPension>28140</ReducedPension>	REDUCED PENSION	VARCHAR
65	<ReducedPension_Date>2017-11-01</ReducedPension_Date>	REDUCED PENSION DATE	DATE
66	<Attd_Allow>0</Attd_Allow>	CONSTANT ATTENDANCE ALLOWANCE	VARCHAR
67	<Comm_Val>1844634</Comm_Val>	COMMUTATION VALUE	VARCHAR
68	<CVP_Date>2017-11-01</CVP_Date>	COMMUTATION VALUE PES DATE	DATE
69	<Arrears>0</Arrears>	ARREARS	VARCHAR
70	<Arrear_From>NA</Arrear_From>	ARREAR FROM	DATE
71	<Arrear_To>NA</Arrear_To>	ARREAR TO	DATE
72	<Penalty_From>NA</Penalty_From>	PENALTY FROM	DATE
73	<Penanlt_To>NA</Penanlt_To>	PANALTY TO	DATE
74	<Penalty_RateOf />	PEANALTY RATE OF	VARCHAR
75	<Penalty_Reason />	PEANALTY REASON	VARCHAR

76	<CV_PaidBy>P</CV_PaidBy>	COMMUTATION VALUE PAID BY (P- PAID BY PAO, N- NOT OPTED, A- TO BE PAID BY BANK)	VARCHAR
77	<Any_Oth_Pension />	ANY OTHER PENSION	VARCHAR
78	<FPName>Sunita </FPName>	FAMILY PENSIONER NAME	VARCHAR
79	<Relationship>Wife</Relationship>	RELATIONSHIP OF FAMILY PENSIONER	VARCHAR
80	<DOB>1965-07-15</DOB>	DATE OF BIRTH	DATE
81	<Nationality>INDIA</Nationality>	NATIONALITY OF FAMILY PENSIONER	VARCHAR
82	<Address>Village Tikari, P.O Kanti (Jasra) ,ALLAHABAD,232307</Address>	ADDRESS OF FAMILY PENSIONER	VARCHAR
83	<Enhanced_RateFP>46900</Enhanced_RateFP>	ENHANCE RATE OF FAMILY PENSIONER	VARCHAR
84	<Enhanced_RateFP_From>NA</Enhanced_RateFP_From>	ENHANCE RATE OF FAMILY PENSIONER FROM	DATE
85	<Enhanced_RateFP_To>2024-10-07</Enhanced_RateFP_To>	ENHANCE RATE OF FAMILY PENSIONER TO	DATE
86	<Normal_RateFP>28140</Normal_RateFP>	FAMILY PENSIONER NORMAL RATE	VARCHAR
87	<Normal_RateFP_From>2024-10-08</Normal_RateFP_From>	FAMILY PENSIONER NORMAL RATE FROM	DATE
88	<Normal_RateFP_To>NA</Normal_RateFP_To>	FAMILY PENISONER NORMAL RATE TO	DATE
89	<Any_Oth_FPen_Dtls>NA</Any_Oth_FPen_Dtls>	ANYOTHER FAMILY PENSION DETAILS	VARCHAR
90	<Iden_Mark>Black mole at chin,</Iden_Mark>	PENSIONER INDETIFICATION MARKS	VARCHAR
91	<FP_Iden_Mark>Mole in the middle of the chin</FP_Iden_Mark>	FAMILY PENSIONER INDETIFICATION MARKS	VARCHAR
92	<FP_Name />	FAMILY PENSIONER NAME(DISABLED)	VARCHAR
93	<GuardianName />	GUARDIAN NAME FOR DISABLED	VARCHAR
94	<DOB_FP />	DATE OF BIRTH FAMILY PENSIONER (DISABLED)	DATE
95	<Rel_Deceased />	REALATIONSHIP OF DECEASED (DISABLED)	VARCHAR
96	<PermanentAddress />	PERAMANENT ADDRESS OF FP (DISABLED)	VARCHAR
97	<Iden_Mark_FP />	IDENTIFICATION MARK OF FAMILY PENSIONER (DISABLED)	VARCHAR
98	<PayCommission>7</PayCommission>	PAY COMMISION	VARCHAR
99	<DRAllowed />	DEARNESS ALLOWED	VARCHAR
100	<DRAllow_Desc />	DEARNESS ALLOW DESCRIPTION	VARCHAR
101	<UT_Attach>Y</UT_Attach>	UNDER TAKING ATTCHED	VARCHAR
102	<PAOCode>033195</PAOCode>	PAO CODE(PAY AND ACCOUNT OFFICE) CODE	VARCHAR
103	<FamilyMember>	FAMILY MEMBER	VARCHAR
104	<FM_Name>Sunita </FM_Name>	FAMILY MEMBER NAME	VARCHAR
105	<RelationshipDesc>Wife</RelationshipDesc>	RELATIONSHIP DESCRIPTION	VARCHAR
106	<FamilyDateOfBirth>1965-07-15</FamilyDateOfBirth>	FAMILY DATE OF BIRTH	DATE
107	<FamilyNationality>INDIA</FamilyNationality>	FAMILY NATIONALITY	VARCHAR
108	<MaritalStatus>Married</MaritalStatus>	MARITAL STATUS	VARCHAR
109	<IsDisabled>N</IsDisabled>	DISABILITY (Y/N)	VARCHAR

 # These fields have case specific value i.e. the value of these fields will be Mandatory in

some pension categories/PPO's and will be non-mandatory in some pension categories/PPO's . Following is the description of abbreviations of categories falling under case specific:

- **FF: Freedom Fighter (Pension Category).**
- **SP: Superannuation Pension (Pension Category).**
- **FP: Family Pension (Pension Category).**
- **MP: MPLOK, MPRAJ (PPO Types).**
- **VR: Voluntary Retirement.**

Details of Family Member Eligible for family pension in the event of death of pensioner.

SL NO.	XML TAGS	DESCRIPTION	DATATYPE
1	<FamilyMember>	FAMILY MEMBER	VARCHAR
2	<FM_Name>Sunita </FM_Name>	FAMILY MEMBER NAME	VARCHAR
3	<RelationshipDesc>Wife</RelationshipDesc>	RELATIONSHIP DESCRIPTION	VARCHAR
4	<FamilyDateOfBirth>1965-07-15</FamilyDateOfBirth>	FAMILY DATE OF BIRTH	DATE
5	<FamilyNationality>INDIA</FamilyNationality>	FAMILY NATIONALITY	VARCHAR
6	<MaritalStatus>Married</MaritalStatus>	MARITAL STATUS	VARCHAR
7	<IsDisabled>N</IsDisabled>	DISABILITY (Y/N)	VARCHAR

Data will be in ASCII format. The details of presenting data in text file are as under:-

1. **Fields will be in the same order as described in the format above.**
2. **One record will be in one line only. This means that if there 100 records, then the text file will contain exactly 100 lines. One record will not be continued in more than one line in text file.**
3. **Date will be sent in character format (YYYYMMDD). For example 01/10/2001 will be send as "20011001"**

Annexure-II eSSA(ePPO)

S.No.	XML TAG NAME	DESCRIPTION
1	<PPO_NUM>	PPO NUMBER
2	<DIARY_NO>	DIARY NUMBER
3	<SSA_NO>	SPECIAL SEAL AUTHORITY(SSA) NUMBER
4	<PEN_NAME>	PENSIONER NAME
5	<REMARKS>	REMARKS
6	<PEN_PPO_BOOK_HANDED>	PENSIONER COPY OF PPO BOOKLET GIVEN BY (B- TO BE GIVBEN BY BANK AND UNDER TAKING IS TO BE TAKEN BY BANK, H- HANDED OVER TO PENSIONER BY HEAD OF OFFICE AND UNDER TAKING IS ATATCHED)
7	<COMM_V>	AMOUNT OF COMMUTATION TO BE PAID BY BANK
8	<PAYING_BRANCH_NAME>	PAYING BRANCH NAME
9	<STNY_NO>	SPECIAL SEAL AUTHORITY AUTHORITY PRINT STATIONARY NUMBER
10	<ADDR_1>	PENSIONER ADDRRSS LINE1
11	<ADDR_2>	PENSIONER ADDRRSS LINE2
12	<ADDR_3>	PENSIONER ADDRRSS LINE3 - STATE (IS BEING CHANGED FROM CODE TO DESCRIPTION)
13	<PEN_PIN>	PIN CODE O FPENSIONER ADDRESS
14	<BASIC_PEN>	BASIC PENSION
15	<BP_START_DATE>	BASIC PENSION START DATE
16	<PEN_AFTR_COMM>	REDUCED PENSION AFTER COMMUTATION
17	<COMMUTATION_PAID_BY>	COMMUTATION PAID BY i.e. TO BE PAID BY BANK, PAID BY PAO, NOT APPLICABLE.
18	<RED_PEN_START>	REDUCED PENSION START DATE
19	<ENFP_RATE>	ENHANCED FAMILY PENSION RATE
20	<FRM_ENFP>	ENHANCED FAMILY PENSION START DATE FROM (BLANK IN CASE OF PENSIONER IS ALIVE)
21	<UPTO_ENFP>	ENHANCED FAMILY PENSION UPTO DATE
22	<ORFP_RATE>	NORMAL FAMILY PENSION RATE
23	<FRM_ORFP>	NORMAL FAMILY PENSION START DATE
24	<UPTO_ORFP>	NORMAL FAMILY PENSION UPTO DATE
25	<LB_ADD1>	CPPC ADDRESS LINE1
26	<LB_ADD2>	CPPC ADDRESS LINE2
27	<LB_ADD3>	CPPC ADDRESS LINE3
28	<LB_PIN_CODE>	CPPC PIN CODE
29	<BANK_DESC>	BANK NAME
30	<PENS_CATEGORY>	PENSION CATEGORY
31	<PAO_NAME>	PAY & ACCOUNTS OFFICE
32	<PAO_ADD1>	PAY & ACCOUNTS OFFICE ADDRESS LINE1
33	<PAO_ADD2>	PAY & ACCOUNTS OFFICE ADDRESS LINE2
34	<PAO_CITY>	PAY & ACCOUNTS OFFICE ADDRESS CITY
35	<PAO_PIN>	PAY & ACCOUNTS OFFICE PINCODE
36	<DATE_PRINT>	SSA PRINT DATE
37	<PEN_ACCOUNT_NO>	PENSIONER ACCOUNT NUMBER
38	<LINE1_LB_ADD>	CPPC ADDRESS TO

39	<ADDITIONAL_PENSION>	ADDITIONAL PENSION
40	<PENSIONER_DOB>	PENSIONER DATE OF BIRTH
41	<PAY_SCALE_COMMISON>	PAY SCALE
42	<NET_QUAL_SERVICE>	NET QUALIFYING SERVICE
43	<DR_REMARK_DISBLTY_AMT>	REMARKS FOR DR ADMISIBLE ON CONSTANT ATTENDANCE ALLOWANCE
44	<CONSTANT_ATTENDANCE_ALLOWANCE>	AMOUNT FOR CONSTANT ATTENDANCE ALLOWANCE
45	<FP_NAME>	FAMILY PENSIONER NAME
46	<FP_DOB>	FAMILY PENSIONER DATE OF BIRTH
47	<LAST_PAY_DRAWN>	LASTE PAY DRAWN
48	<GRADE_PAY>	GRADE PAY
49	<AIS_CODE>	ALL INDIA SERVICE CODE (AIS TYPE/AIS CADRE/ AIS YEAR OF JOIN)
50	<BNK_PAY_CODE>	PAYING BRANCH BSR CODE
51	<PEN_ADHAAR_NO>	PENSIONER ADHAAR NUMBER
52	<PEN_PAN_NO>	PENSIONER PAN NO
53	<PEN_PHONE>	PENSIONER MOBILE NUMBER
54	<MED_AMT>	MEDICAL ALLOWNACE AMOUNT (IF PRESENT PENSIONER HAD NOT OPTED FOR CGHS)
55	<MED_AMT_FRM>	MEDICAL ALLOWANCE FROM DATE
56	<PAY_COM_TXT>	PAY COMMISION
57	<PAY_MATRIX>	PAY MATRIX (LEVEL: , INDEX:)
58	<PEN_EMAIL>	PENSIONER EMAIL
59	<NPA>	NPA AMOUNT (DOCTORS)
60	<DEATH_IN_HARNESS_FLAG>	ON DUTY DEATH FLAG (IF YES THEN ENHANCED PERIOD IS 10 YEARS ISNTEAD OF 7 YEARS)
61	<DATE_RET>	DATE OF RETIREMENT
62	<DATE_DEATH>	DATE OF DEATH
63	<GENDER>	GENDER OF PENSIONER
64	<PAYING_BRANCH_BSR>	PAYING BRANCH BSR CODE
65	<LINK_CPPC_BSR>	CPPC BSR CODE
66	<PAO_CODE>	PAO CODE
67	<IFSC_CODE>	IFSC CODE
68	<PEN_DEBIT_FOR>	To Identify PAO Delhi Cases And AIS cases Separate Payment Scrolls may be prepared and submitted to RBI and CPAO. : For AIS Cases Debit able to Consolidated Fund of Delhi- Bank/RBI to prepare separate scroll and put through : For PAO Delhi Cases

Annexure-III XML

Sample of ePPO

<EPPONo xmlns="http://webservices.pfms.nic.in/PFMSExternalWebService.xsd">
<PPONO>331951700524</PPONO>
<PPODate>2017-10-23</PPODate>
<DiaryNumber>W03319517100001</DiaryNumber>
<ClassOfPension>A</ClassOfPension>
<PensionHead>2071</PensionHead>
<SubMajorHead>1</SubMajorHead>
<MinorHead>101</MinorHead>
<Votedcharged>Voted</Votedcharged>
<FileNo>233212\2017\1</FileNo>
<BankName>CORPORATION BANK</BankName>
<BankBSRCode>0350385</BankBSRCode>
<IFSCCODE>HDFC0001668</ IFSCCODE >
<BankAddress>NEW DELHI-LODHI COMPLEX GROUND FLOOR, BLOCK II, CGO COMPLEX PHASE I 110003</BankAddress>
<Accountno>037100101024892</Accountno>
<PSName>Mr. GANGA PRASAD </PSName>
<Adhaarno />
<PAN>ADMPP4337L</PAN>
<Email>ganga.prasad@nic.in</Email>
<MobileNo>9810207415</MobileNo>
<DDOCode>233212</DDOCode>
<RetiredFrom>DDO, NIC,(Headquarters), DELHI</RetiredFrom>
<Group>A</Group>
<Designation>DEPUTY DIRECTOR</Designation>
<PermanentAddress1>Village Tikari, P.O Kanti (Jasra) </PermanentAddress1>
<PermanentDistrict>ALLAHABAD</PermanentDistrict>
<PermanentState>UTTAR PRADESH</PermanentState>
<PermanentPinCode>232307</PermanentPinCode>
<Naitionality>INDIA</Naitionality>
<Gender>M</Gender>
<DateOfBirth>1957-10-08</DateOfBirth>
<JoiningDate>1981-12-07</JoiningDate>
<RetirementDate>2017-10-31</RetirementDate>
<DateOfDeath>1900-01-01</DateOfDeath>
<QS_YEAR>35</QS_YEAR>
<QS_MONTH>10</QS_MONTH>
<QS_DAY>25</QS_DAY>
<NQS_YEAR>00</NQS_YEAR>
<NQS_MONTH>01</NQS_MONTH>
<NQS_DAY>17</NQS_DAY>
<AQS_YEAR>00</AQS_YEAR>
<AQS_MONTH>00</AQS_MONTH>
<AQS_DAY>00</AQS_DAY>
<TQS_YEAR>35</TQS_YEAR>
<TQS_MONTH>09</TQS_MONTH>
<TQS_DAY>08</TQS_DAY>
<TotalQualifyingService>350908</TotalQualifyingService>
<LastPayDrawn>93800</LastPayDrawn>
<PayScale>67700-208700</PayScale>
<AvgEmol>93800</AvgEmol>
<EmolFamilyPension>93800</EmolFamilyPension>

<EmolRGDG>98490</EmolRGDG>
<ExGratiaPayment>0</ExGratiaPayment>
<NPA>0</NPA>
<AnyOtherPay>0</AnyOtherPay>
<Level>11</Level>
<Index>12</Index>
<GradePay>0</GradePay>
<Med_Allow />
<Med_Date>1900-01-01</Med_Date>
<RGDGNotByBank>1625085</RGDGNotByBank>
<PensionAmount>46900</PensionAmount>
<DateofCommencement>2017-11-01</DateofCommencement>
<AmountCommuted>18760</AmountCommuted>
<DateOfRestoration>On completion of 15 years of reduced monthly pension after commutation</DateOfRestoration>
<ReducedPension>28140</ReducedPension>
<ReducedPension_Date>2017-11-01</ReducedPension_Date>
<Attd_Allow>0</Attd_Allow>
<Comm_Val>1844634</Comm_Val>
<CVP_Date>2017-11-01</CVP_Date>
<Arrears>0</Arrears>
<Arrear_From>NA</Arrear_From>
<Arrear_To>NA</Arrear_To>
<Penalty_From>NA</Penalty_From>
<Penanlt_To>NA</Penanlt_To>
<Penalty_RateOf />
<Penalty_Reason />
<CV_PaidBy>P</CV_PaidBy>
<Any_Oth_Pension />
<FPName>Sunita </FPName>
<Relationship>Wife</Relationship>
<DOB>1965-07-15</DOB>
<Nationality>INDIA</Nationality>
<Address>Village Tikari, P.O Kanti (Jasra) ,ALLAHABAD,232307</Address>
<Enhanced_RateFP>46900</Enhanced_RateFP>
<Enhanced_RateFP_From>NA</Enhanced_RateFP_From>
<Enhanced_RateFP_To>2024-10-07</Enhanced_RateFP_To>
<Normal_RateFP>28140</Normal_RateFP>
<Normal_RateFP_From>2024-10-08</Normal_RateFP_From>
<Normal_RateFP_To>NA</Normal_RateFP_To>
<Any_Oth_FPen_Dtls>NA</Any_Oth_FPen_Dtls>
<Iden_Mark>Black mole at chin,</Iden_Mark>
<FP_Iden_Mark>Mole in the middle of the chin</FP_Iden_Mark>
<FP_Name />
<GuardianName />
<DOB_FP />
<Rel_Deceased />
<PermanentAddress />
<Iden_Mark_FP />
<PayCommission>7</PayCommission>
<DRAllowed />
<DRAllow_Desc />
<UT_Attach>Y</UT_Attach>
<PAOCode>033195</PAOCode>
<FamilyMember>

<FM_Name>Sunita </FM_Name>
<RelationshipDesc>Wife</RelationshipDesc>
<FamilyDateOfBirth>1965-07-15</FamilyDateOfBirth>
<FamilyNationality>INDIA</FamilyNationality>
<MaritalStatus>Married</MaritalStatus>
<IsDisabled>N</IsDisabled>
</FamilyMember>
<FamilyMember>
<FM_Name>Pramod Kumar </FM_Name>
<RelationshipDesc>Son</RelationshipDesc>
<FamilyDateOfBirth>1981-06-13</FamilyDateOfBirth>
<FamilyNationality>INDIA</FamilyNationality>
<MaritalStatus>Married</MaritalStatus>
<IsDisabled>N</IsDisabled>
</FamilyMember>
<FamilyMember>
<FM_Name>Vinod Kumar Prasad</FM_Name>
<RelationshipDesc>Son</RelationshipDesc>
<FamilyDateOfBirth>1986-01-19</FamilyDateOfBirth>
<FamilyNationality>INDIA</FamilyNationality>
<MaritalStatus>Married</MaritalStatus>
<IsDisabled>N</IsDisabled>
</FamilyMember>
<FamilyMember>
<FM_Name>Manoj Kumar </FM_Name>
<RelationshipDesc>Son</RelationshipDesc>
<FamilyDateOfBirth>1987-10-28</FamilyDateOfBirth>
<FamilyNationality>INDIA</FamilyNationality>
<MaritalStatus>Married</MaritalStatus>
<IsDisabled>N</IsDisabled>
</FamilyMember>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
<Reference URI="">
<Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<DigestValue>QbG3TFRh7doyBh69NKoL4jarZZ0=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>YhiFkkXdp61V0QJ/XO5qEU6XHmkgd+7iVbKyyP+5PRWLXBc9pMYJ+P9aOzTVnY/z/G2WvZdc2xCB3uHchVJ6eCrA37sD79kDFS1cQq2tcDV54kFDntX2RhRIO03V9WJAMgG4LNU6o+7BjRsqEp47vj/gHriDp9o7Ua6Zs8cq01NcyL8M2kO21lliWJ6d0en4zRyxJ7fRMN3TEda/fhB94PHVB7MiJg992TpObvR46NdKNGg5dmYDwzE7wOS7ualZs6E2yePNAySO+a6lSMVWLOhOt7H34/chJMcZ0xjQLMqcPcDJQYzyRK3Y+Xj4zUI5YfwHNvmQ0q5n8ywcQAF0Dg==</SignatureValue>
<KeyInfo>
<X509Data>
<X509IssuerSerial>
<X509IssuerName>CN=(n)Code Solutions CA 2014, OID.2.5.4.51="301, GNFC Infotower", STREET="Bodakdev, S G Road, Ahmedabad", ST=Gujarat,

OID.2.5.4.17=380054, OU=Certifying Authority, O=Gujarat Narmada Valley Fertilizers and Chemicals Limited, C=IN</X509IssuerName>
<X509SerialNumber>1398372578</X509SerialNumber>
</X509IssuerSerial>
<X509Certificate>MIIHCjCCBfKgAwIBAgIEU1l44jANBgkqhkiG9w0BAQsFADCB/DE
LMAkGA1UEBhMCSU4xQTA/BgNVBAoTOEd1amFyYXQgTmFybWFkYSBWYWxsZ
XkgRmVydGlsaXplcnMgYW5kIENoZW1pY2FscyBMaW1pdGVkMR0wGwYDVQQLE
xRDZXJ0aWZ5aW5nIEF1dGhvcml0eTEPMA0GA1UEERMGMzgwMDU0MRAwDgY
DVQQIEwdHdWphcmF0MSYwJAYDVQQJEx1Cb2Rha2RldiwgUyBHIFJvYWQsIEFo
bWVkYWJhZDEcMBoGA1UEMxMTMzAxLCBHTkZDIEluZm90b3dlcjEiMCAGA1UEA
xMZKG4pQ29kZSBTb2x1dGlvbnMgQ0EgMjAxNDAeFw0xNzAxMTgxMDA0MTNaFw
0xOTAxMTgwODI1MzlaMIHjMQswCQYDVQQGEwJJTjEqMCgGA1UEChMhTkFUS
U9OQUwgSU5GT1JNQVRJQ1MgQ0VOVFJFIChQQU8pMUkwRwYDVQQUE0BkM
DM5NmNjZmM0N2NjNDUwYWIzYjllZTY5YzRlYTQxZWNjZDhlM2VjMmNlNDU5Ym
NkNGM0NmE2ODUwYjFlODUzMSQwIgYDVQQLExtOSUMgTWluLm9mLklULEVDS
UQgLSA5ODM4MjgxDzANBgNVBBETBjExMDAwMzEOMAwGA1UECBMFRGVsaG
kxFjAUBgNVBAMTDVNVTUFOIENISEFCUkEwggEiMA0GCSqGSIb3DQEBAQUAA
4IBDwAwggEKAoIBAQC9/FmHJmP4kwKw7fsPBRFZuP+3J1tFyubp2x7JjoeN/VX74
Bd9mPx/mab60YIdNySvT7NHAFC4MMcNQiBa9qdLdA2RS95qrTBVA0RBNU4yxnn
70F2r25xi7l6I6cZaYSSlZxWe+zubUOvBUgt00Oxk8rLnRY+5FDGoyQOKbyXwDapN
dyVJsEjxGYrsDasX7wUoI+3tlfS2ZDGnxgr/j9raN8CBBOnu16h4n+vrriwpuFYZ/uaiG/f
R7vEO8R9g8PVE4ULQkT29xsPa9LijYnfN7NVnM3bH/HkbIHSusAYu0VG38vY6+3Q
HBNPp3dx6G9MKjSjTPQMN1xuOhcSql4gvAgMBAAGjggKpMIICpTAOBgNVHQ8BA
f8EBAMCBSAwZAYDVR0gBF0wWzBZBgZggmRkAgIwTzBNBggrBgEFBQcCAjBBG
j9DbGFzcyAyIGNlcnRpZmljYXRlcyB1c2VkIGZvciBlbmNyeXB0aW5nIGxvdyByaXNrI
HRyYW5zYWN0aW9ucy4wUQYIKwYBBQUHAQEERTBDMEEGCCsGAQUFBzAChj
VodHRwczovL3d3dy5uY29kZXNvbHV0aW9ucy5jb20vcmVwb3NpdG9yeS9uY29kZ
WNhLmNlcjAZBgNVHREEEjAQgQ5jLnN1bWFuQG5pYy5pbjCCAW4GA1UdHwSCA
WUwggFhMIIBHqCCARqgggEWpIIBEjCCAQ4xCzAJBgNVBAYTAklOMUEwPwYDV
QQKEzhHdWphcmF0IE5hcm1hZGEgVmFsbGV5IEZlcnRpbGl6ZXJzIGFuZCBDaGV
taWNhbHMgTGltaXRlZDEdMBsGA1UECxMUQ2VydGlmeWluZyBBdXRob3JpdHkx
DzANBgNVBBETBjM4MDA1NDEQMA4GA1UECBMHR3VqYXJhdDEmMCQGA1UE
CRMdQm9kYWtkZXYsIFMgRyBSb2FkLCBBaG1lZGFiYWQxHDAaBgNVBDMTEzM
wMSwgR05GQyBJbmZvdG93ZXIxIjAgBgNVBAMTGShuKUNvZGUgU29sdXRpb25z
IENBIDIwMTQxEDAOBgNVBAMTB0NSTDI5NjIwPaA7oDmGN2h0dHBzOi8vd3d3L
m5jb2Rlc29sdXRpb25zLmNvbS9yZXBvc2l0b3J5L25jb2RlY2ExNC5jcmwwEwYDVR
0jBAwwCoAITQe+8Z6d+70wHQYDVR0OBBYEFDe/luW6/rthWgKX4iMObGz9l48lM
BkGCSqGSIb2fQdBAAQMMAobBFY4LjEDAgMoMA0GCSqGSIb3DQEBCwUAA4IB
AQBjVJN7oXaR/qJThk7hZpBWB6H/RbsbTY8hyOU33Zr1p7alX8Ag1xncYdf+XO+CX
+QT8jdDyWxVAEm/O0AiuuktdY+XFkwJOWD5tfWDOe214yg2EE3KS65XH3B02TvF
/AVUBi5I4nXMmaC1LAzzNQPlUfFU9P2LuoDILqxqi0SNL+4B2PIFNhcPEus7jHNUjB
I+n0/Wz2YY2CVDyos3DKS2xmyJIG+ET+fyZ1jKTAU5govB0Ml9iIIOZTAaFYsJlvdH
mstXZe13sVHhGM8lxnynA9jhh4RQ1qG2Kt0oL6nGBs2R1yu+uvWBnpTXagk5FjPxZ
zTjK/GZmXRWGwSk4ES1</X509Certificate>
</X509Data>
</KeyInfo>
</Signature>
</EPPONo>

Annexure-IV
XML Sample of eSSA(Amendment)

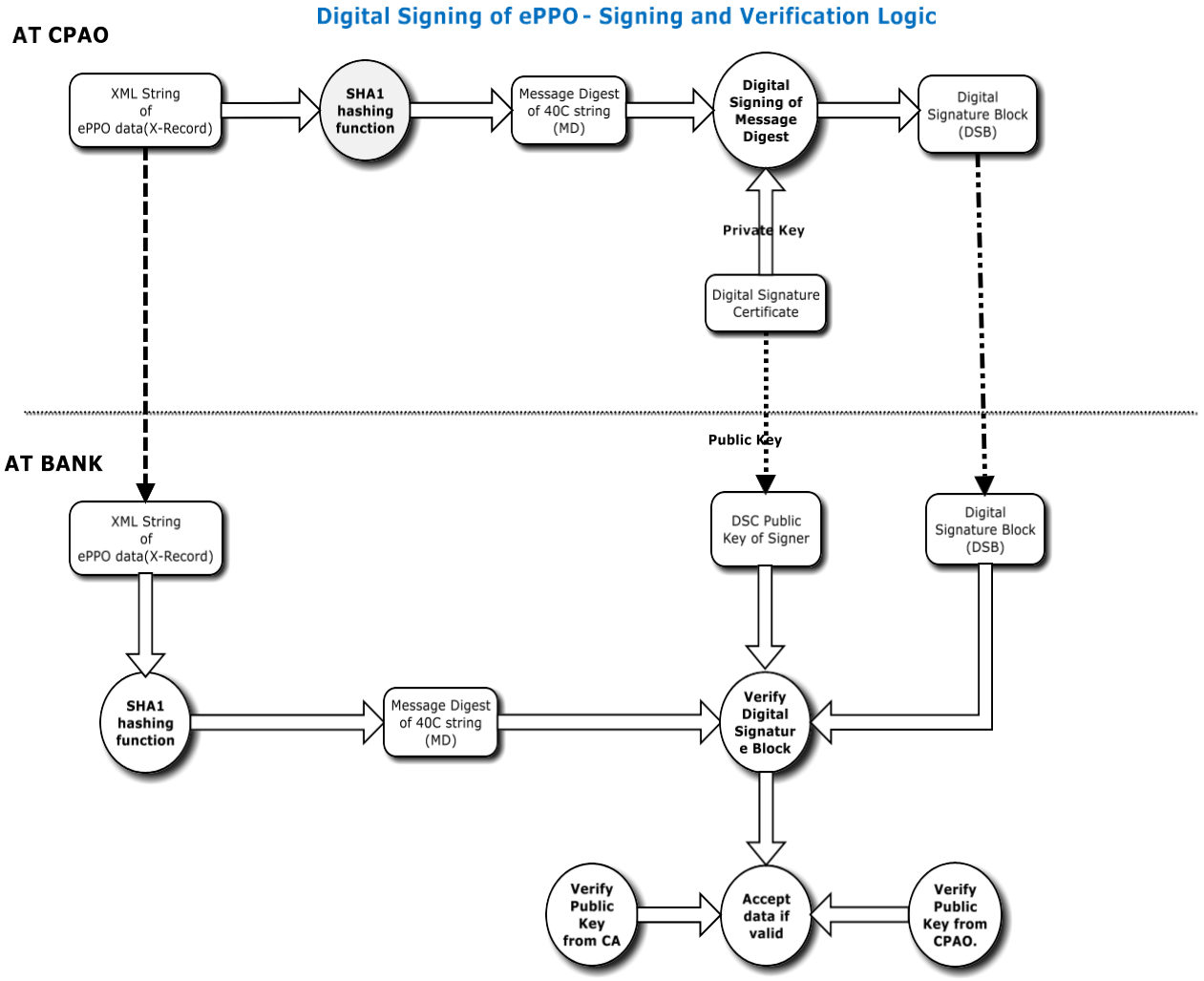

```
<SSA>
  <ROWSET>
    <NEWPPO num="1">
      <PPO_NUM>078151700359</PPO_NUM>
      <DIARY_NO>PN117009296</DIARY_NO>
      <SSA_NO>1090336</SSA_NO>
      <PEN_NAME>Mr. ARUN KUMAR SHARMA</PEN_NAME>
      <REMARKS>7. </REMARKS>
      <PEN_PPO_BOOK_HANDED>B</PEN_PPO_BOOK_HANDED>
      <PAYING_BRANCH_NAME>PUSHPANJALI ENCLAVE,B-96, PUSHPANJALI
ENCLAVE, PITAM PURA,,NEW DELHI, DELHI</PAYING_BRANCH_NAME>
      <STNY_NO>CC072159A</STNY_NO>
      <ADDR_1>B- 53 PUSHPANJALI ENCLAVE </ADDR_1>
      <ADDR_2>PITAM PURA </ADDR_2>
      <ADDR_3>DELHI</ADDR_3>
      <PEN_PIN>110034</PEN_PIN>
      <BASIC_PEN>30200</BASIC_PEN>
      <BP_START_DATE>01/08/2017</BP_START_DATE>
      <PEN_AFTR_COMM>18120</PEN_AFTR_COMM>
      <COMMUTATION_PAID_BY>PAID BY PAO</COMMUTATION_PAID_BY>
      <RED_PEN_START>01/08/2017</RED_PEN_START>
      <ENFP_RATE>30200</ENFP_RATE>
      <UPTO_ENFP>10/07/2024</UPTO_ENFP>
      <ORFP_RATE>18120</ORFP_RATE>
      <FRM_ORFP>11/07/2024</FRM_ORFP>
      <UPTO_ORFP>Till Death/ReMarriage</UPTO_ORFP>
      <LB_ADD1>CENTRALISED PENSION PROCESSING CENTRE,</LB_ADD1>
      <LB_ADD2>CHANDNI CHOWK,</LB_ADD2>
      <LB_ADD3>DELHI</LB_ADD3>
      <LB_PIN_CODE>PIN-110006</LB_PIN_CODE>
      <BANK_DESC>STATE BANK OF INDIA</BANK_DESC>
      <PENS_CATEGORY>SUPERANNUATION PENSION</PENS_CATEGORY>
      <PAO_NAME>PAO(Textile), NewDelhi</PAO_NAME>
      <PAO_ADD1>529, UDHYOG BHAWAN</PAO_ADD1>
      <PAO_CITY>NEW DELHI</PAO_CITY>
      <PAO_PIN>PIN-</PAO_PIN>
      <DATE_PRINT>06/09/2017</DATE_PRINT>
      <PEN_ACCOUNT_NO>36405021209</PEN_ACCOUNT_NO>
      <LINE1_LB_ADD>THE MANAGER</LINE1_LB_ADD>
      <ADDITIONAL_PENSION>AS APPLICABLE</ADDITIONAL_PENSION>
      <PENSIONER_DOB>11/07/1957</PENSIONER_DOB>
      <NET_QUAL_SERVICE>35 - 01 - 00 </NET_QUAL_SERVICE>
      <FP_NAME>Mrs. SAROJ SHARMA</FP_NAME>
      <FP_DOB>08/07/1960</FP_DOB>
      <LAST_PAY_DRAWN>Rs.60400/-</LAST_PAY_DRAWN>
      <BNK_PAY_CODE>0016238</BNK_PAY_CODE>
      <PEN_ADHAAR_NO>840111459338</PEN_ADHAAR_NO>
      <PEN_PAN_NO>AGOPS7715A</PEN_PAN_NO>
      <PEN_PHONE>9868879301</PEN_PHONE>
      <PAY_COM_TXT>AS PER 7 CPC</PAY_COM_TXT>
      <PAY_MATRIX>(Level:7, INDEX:11)</PAY_MATRIX>
      <DEATH_IN_HARNESS_FLAG>N</DEATH_IN_HARNESS_FLAG>
```

<DATE_RET>31/07/2017</DATE_RET>
<GENDER>M</GENDER>
<PAYING_BRANCH_BSR>0016238</PAYING_BRANCH_BSR>
<LINK_CPPC_BSR>0004475</LINK_CPPC_BSR>
<PAO_CODE>P075305</PAO_CODE>
<IFSC_CODE>HDFC0001668</IFSC_CODE>
<PEN_DEBIT_FOR> Debit able to Consolidated Fund of Delhi- Bank/RBI to prepare separate scroll and put through </PEN_DEBIT_FOR>
</NEWPPO>
</ROWSET>
<Signature_Node>
<Serial_No>5349A9D1</Serial_No>
<Signed_By>DILIP PATHAK</Signed_By>
<Valid_Till>8/30/2018 5:15:21 PM</Valid_Till>
<Version>Version=1.0, Release Date=05/11/2014</Version>

<Msg_Digest>o1nYRQucRNViNLZAzLTXxjoxsCsLZ4/QJr2H4QdgjOIk/czpKi0lXfhBFnFnovQs
rfByc+OU20pH6Mg3wbxUZQO24XP0hOhNwZAg5FmFJqdcq/d2RQAbXKliXenghHP7fif+tPC
KCGSsEusISdbSfay0X5ClifO3SDCxO3vZPOlyVU0cAo7enN2PwLpgfIsTkIlwCqeVbuC+FyAJ
pSvPGbcBwmOsmKiiPjUx29WGCld7+feKyG2CzmrV8N/GQwdAF22kGuMjsgJBUHof/RBMO
5UA+/Zm24SUlRIrWK6wla7AXV6A1kgontlYusbr4IVSojk7mQjqXKj4OUX7dF9lYQ==</Msg_D
igest>
</Signature_Node>
</SSA>

Annexure-V

Digital Signing Logic



Signing Algorithm

1. Generate xml string from data corresponding to new ppo or revision authority as the case may be.
2. Generate hash code for this string by subjecting this xml string to some hashing function like SHA1. This hash code will act as our message digest.
3. Sign this message digest with the private key of signer, which will result in signed message.
4. We need to send the following to the receiver as mandatory parameters.
    - XML data string (record itself)
    - Name of hashing function (SHA1 in this case)
    - Signed Message Digest
    - Public Key
        - Modulus
        - Exponent

Verification Algorithm

5. Extract the record from xml file contained within the tags named <NEWPPO>
6. From this record extract all the elements with data as string, contained within the tags <DATA_BLOCK> and </DATA_BLOCK>, but do not include these tags in the string. Let us call this string as Data_String.
7. Subject this Data_string to hashing function which is mentioned in the XML record within the tags <HASH_FUNCTION></HASH_FUNCTION>. Normally it is SHA1. If it is SHA1 then 40 character hash code will be generated. Let us call it as Message Digest MD_Str.
8. Extract Public_Key Modulus from <DSC_PUBLICKEY_MODULUS>
9. Extract Public_Key Exponent from <DSC_PUBLICKEY_EXPONENT>
10. Extract Signed Message Digest from <XML_SIGN>
11. Suject these three parameters for signature verification.
    1. Message Digest MD_Str
    2. Signed Message Digest XML_Signature
    3. Public Key
        a. Modulus
        b. Exponent

If it gets verified then data received is valid one.

Logic to Validate Digitally Signed eSSA (EPPO) XML File of CPAO

```
<SSA>
        <ROWSET>
                <NEWPPO num="1">
                        --SSA DATA
                </ NEWPPO >
        </ROWSET>

                        <Signature_Node>
                                <Serial_No>
                        --Serial No of Digital Certificate
                </Serial_No>
                <Signed_By>
                        --Name of The Person who Signed it
                </Signed_By>
                <Valid_Till>
                        -- Validatity of Digital Signature
                </Valid_Till>
                <Version>
                        --Software Version 6.0 For EPPO Cases
                </Version>
                <Msg_Digest>
                        --Digitally Signed HASH
                </Msg_Digest>
                        </Signature_Node>
</SSA>
```

Structure of Digitally Signed XML

How to read Digitally Signed XML

Step 1: Read <ROWSET> </ROWSET>

Step 2: Calculate SHA1 Hash of <ROWSET> </ROWSET>

Step 3: Use the Public Key Available at CPAO.NIC.IN in BANK LOGIN, Match the serial No <Serial_no> </Serial_no> with the Keys Available. Please Note These Keys can be installed in your X509 Store.

Step 4: Read Value <Msg_Digest> </Msg_Digest>

Step 5: Match the Calculated HASH of Step 2 + Public Key with Data from Step 4

.Net (C#) Code Sample to Demonstrate how to Validate a Digitally Signed XML

```
//.NET C# Button Click Event Code to verify Signed XML Document private void
        SignVerify_Click(object sender, EventArgs e)
        {
            try
```

```
            {

                //Load Signed XML Document
                XmlDocument origSignedXml = new XmlDocument();

                //Change Environment.GetEnvironmentVariable("TEMP")
+ @"\Signed.xml" with Correct Local Path
                origSignedXml.Load(Environment.GetEnvironmentVariable("TEMP") +
@"\" + PPODairyNo + "Signed.xml");

                //Extract Only Data Part From Signed XML

                DocumnetXmlDocument final = new XmlDocument();
                XmlNode recnod =
final.ImportNode(origSignedXml.DocumentElement.SelectSingleNode("/SSA/ROWSET"),
true);
                final.LoadXml(recnod.OuterXml.ToString());
                final.Save(Environment.GetEnvironmentVariable("TEMP") + @"p2.xml");


                //          Read Only Message Digest From Signed XML
                Document XmlDocument oo = new XmlDocument();

                //Change Environment.GetEnvironmentVariable("TEMP")
+ @"\Signed.xml" with Correct Local Path oo.Load(Environment.GetEnvironmentVariable("TEMP")
                + @"\Signed.xml"); XmlNode recnod1 =
oo.DocumentElement.SelectSingleNode("/SSA/Signature_Node/Msg_Digest");

                //Local Path Of Certifiacte's Public Key
                string CerPath = @"d:\pub1.cer";

                    //Verify Data Part, Calls Verify() Method With Required Parameters if
                (Verify(GetSHA1Hash(Environment.GetEnvironmentVariable("TEMP") +
@"p2.xml"), Convert.FromBase64String(recnod1.InnerText.ToString()), CerPath))
                    MessageBox.Show("Verified !!");
                else
                    MessageBox.Show("Not Verified !!");
            }
            catch (Exception ex)
            {
                MessageBox.Show("Some Error, Contact System Admin!! "
+ ex.Message.ToString());
            }
        }




//Function to verify XML Data
        static bool Verify(string text, byte[] signature, string certPath)
        {

            //Load Public Certificate
            X509Certificate2 cert = new X509Certificate2(certPath);
```

```
            RSACryptoServiceProvider csp =
(RSACryptoServiceProvider)cert.PublicKey.Key;

            // Hash the data
            SHA1Managed sha1 = new SHA1Managed();
            UnicodeEncoding encoding = new UnicodeEncoding(); byte[]
            data = encoding.GetBytes(text); byte[] hash =
            sha1.ComputeHash(data);

            // Verify the signature with the hash
            return csp.VerifyHash(hash,
CryptoConfig.MapNameToOID("SHA1"), signature);
        }


 //Function to get SHA1
            public static string GetSHA1Hash(string pathName)
        {
            string strResult = ""; string
            strHashData = "";

            byte[] arrbytHashValue; System.IO.FileStream
            oFileStream = null;

            System.Security.Cryptography.SHA1CryptoServiceProvider oSHA1Hasher
= new System.Security.Cryptography.SHA1CryptoServiceProvider();

            try
            {
                oFileStream = GetFileStream(pathName);
                arrbytHashValue = oSHA1Hasher.ComputeHash(oFileStream); oFileStream.Close();

                strHashData = System.BitConverter.ToString(arrbytHashValue);
                strHashData
                = strHashData.Replace("-", ""); strResult = strHashData;
            }
            catch (System.Exception ex)
            {
                System.Windows.Forms.MessageBox.Show(ex.Message, "Error!",
System.Windows.Forms.MessageBoxButtons.OK,
System.Windows.Forms.MessageBoxIcon.Error,
System.Windows.Forms.MessageBoxDefaultButton.Button1);
            }

            return (strResult);
        }
```

.Net (C#) Code Sample to demonstrate how to validate a Digitally Signed XML sent on and after 01-Nov-2019.

```
//.NET C# Button Click Event Code to verify Signed XML Document

private void SignVerify_Click(object sender, EventArgs e)
 {
   try
 {
   //Load Signed XML Document
   XmlDocument origSignedXml = new XmlDocument();


   //Change Environment.GetEnvironmentVariable("TEMP") + @"\Signed.xml" with Correct
Local Path

origSignedXml.Load(Environment.GetEnvironmentVariable("TEMP") + @"\" + PPODairyNo
+ "Signed.xml");

   //Extract Only Data Part From Signed XML

Document XmlDocument final = new XmlDocument();
XmlNode recnod=final.ImportNode(origSignedXml.DocumentElement.SelectSingleNode
("/SSA/ROWSET"),true);

    final.LoadXml(recnod.OuterXml.ToString());
    final.Save(Environment.GetEnvironmentVariable("TEMP") + @"p2.xml");

   //Read Only Message Digest From Signed XML

Document XmlDocument oo = new XmlDocument();

   //Change Environment.GetEnvironmentVariable("TEMP") + @"\Signed.xml" with Correct
Local Path

oo.Load(Environment.GetEnvironmentVariable("TEMP") + @"\Signed.xml");
XmlNode recnod1
=oo.DocumentElement.SelectSingleNode("/SSA/Signature_Node/Msg_Digest");

   //Local Path Of Certifiacte's Public Key

string CerPath = @"d:\pub1.cer";

  //Verify Data Part, Calls Verify() Method With Required Parameters

 if (Verify(GetSHA2Hash (Environment.GetEnvironmentVariable("TEMP") + @"p2.xml"),
Convert.FromBase64String(recnod1.InnerText.ToString()), CerPath))
     MessageBox.Show("Verified !!");
    else
       MessageBox.Show("Not Verified !!");
      }
       catch (Exception ex)
      {
        MessageBox.Show("Some Error, Contact System Admin!! " + ex.Message.ToString());
      }
   }
```

```
//Function to verify XML Data

public bool Verify(string text, byte[] signature, string certPath)
{
   X509Certificate2 cert = new X509Certificate2(certPath);
   RSACryptoServiceProvider csp = (RSACryptoServiceProvider)cert.PublicKey.Key;
   // Hash the data
   SHA256Managed sha2 = new SHA256Managed();
   UnicodeEncoding encoding = new UnicodeEncoding();
   byte[] data = encoding.GetBytes(text);
   byte[] hash = sha2.ComputeHash(data);
   // Verify the signature with the hash
   return csp.VerifyHash(hash, CryptoConfig.MapNameToOID("SHA256"), signature);
}
```

```
Function to get SHA2

    public static string GetSHA2Hash(string pathName)
    {
   string strResult = "";
   string strHashData = "";
   byte[] arrbytHashValue;
   System.IO.FileStream oFileStream = null;

   System.Security.Cryptography.SHA256CryptoServiceProvider oSHA1Hasher = new
   System .Security.Cryptography.SHA256CryptoServiceProvider();
     oFileStream = GetFileStream(pathName);
      arrbytHashValue = oSHA1Hasher.ComputeHash(oFileStream);
      oFileStream.Close();
      strHashData = System.BitConverter.ToString(arrbytHashValue);
      strHashData = strHashData.Replace("-", "");
      strResult = strHashData;
   return (strResult);
     }
```

Format of Acknowledgment (XML)

1. **File Name (Nomenclature)** : **ACK-<SAME as of ePPO (Revision) Data file>.xml**

   The Name of file should be same as what file name was received from CPAO but with a prefix 'ACK-'

   E.g. ACK-1724046-20150601.xml

2. **File Structure** :

```
<ACK>
        <PPO_NO></PPO_NO>
        <DIARY_NO></DIARY_NO>
        <SSA_NO></SSA_NO>
        <PROCESSED_DATE></PROCESSED_DATE>
        <PROCESSING_STATUS></PROCESSING_STATUS>
        <PROCESSING_REMARKS></PROCESSING_REMARKS>
</ACK>
```

2.1. TAG Description :

2.1.1. <PPO_NO>: PPO Number of Case Processed.

2.1.2. <DIARY_NO>: Diary Number Associated with PPO number (Already provided by CPAO in ePPO (Revision) Data file).

2.1.3. <SSA_NO>: SSA Number Associated with PPO number (Already provided by CPAO in ePPO (Revision) Data file).

2.1.4. <PROCESSED_DATE>: Date when case was processed by BANK (CPPC).

2.1.5. <PROCESSING_STATUS>: This Tag will only have either of two Value

2.1.5.1. ACCEPTED: in case of successful processing.
2.1.5.2. REJECTED: in case of discrepancy or error.

2.1.6. <PROCESSING_REMARKS>: This is mandatory in case when processing status is 'REJECTED' and description should be given about the error/discrepancy.

Note*:** *The acknowledgment file should be generated individually for all cases received and processed i.e. a file will contain record for only one PPO case,* ***if acknowledgment is not received within 3 days it will be treated as accepted

Annexure-VI

Infrastructure Requirement

CPAO

- Digital signatures are required for all signatories.
- One .Net server is required as .Net technology will be used to digital sign the documents and data.
- Software modules are required to be prepared for digital signing the documents.

Banks

- SFTP server is required at bank end, where files will be uploaded by the CPAO.
- Banks to provide the user name and password for CPAO, to access the SFTP server.
- Banks to prepare software for importing the XML data from CPAO, directly into their CPPC system

Please extract sample files from Files.rar

Files.rar