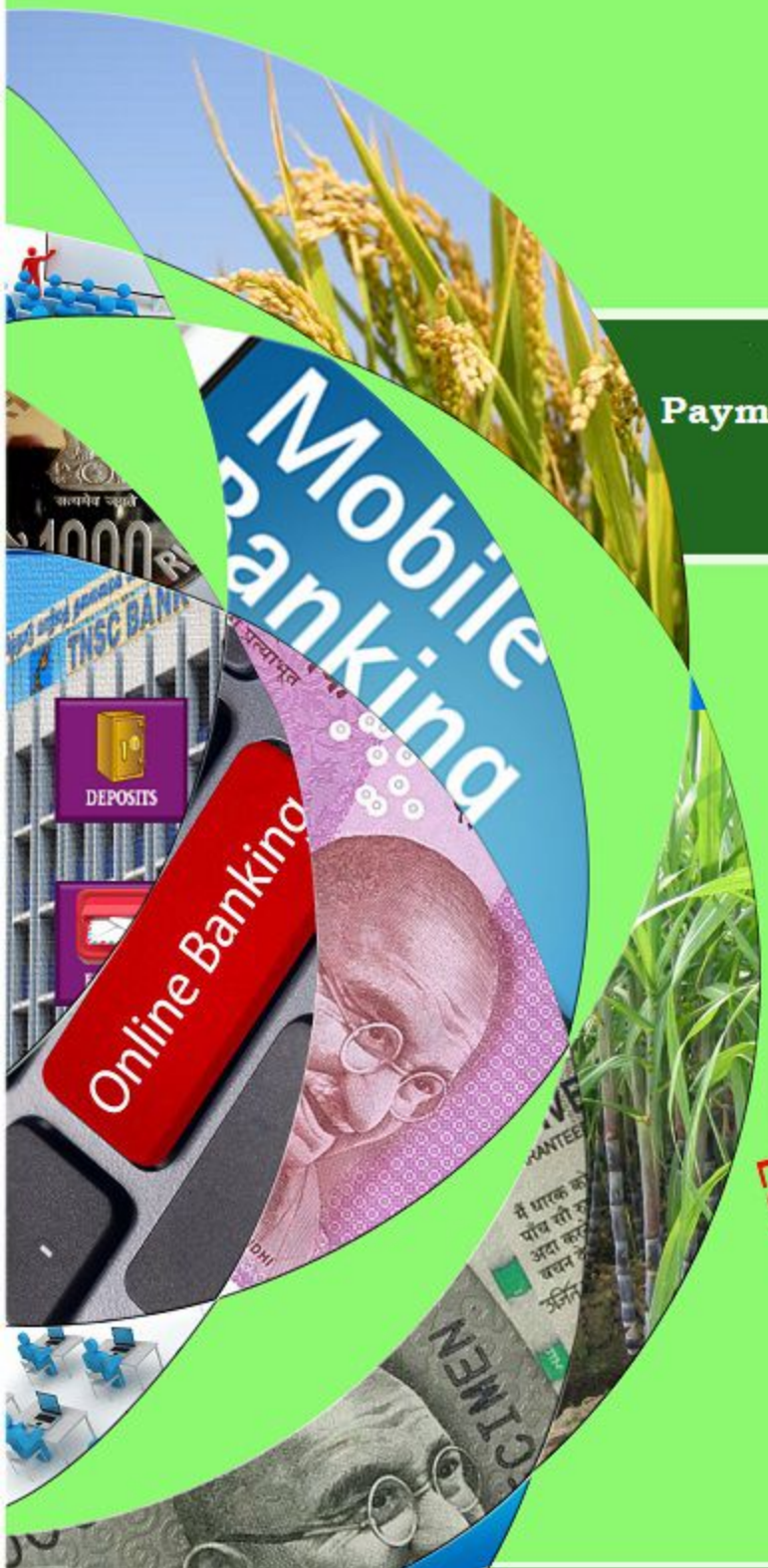
TNSC BANK

Payment System -Online Transactions



Let's do our bit to save our Mother Earth

AGRICULTURAL CO-OPERATIVE STAFF TRAINING INSTITUTE

Sponsored by: THE TAMIL NADU STATE APEX CO-OP. BANK LTD

POST BOX NO.5, OPP. TO AAVIN ILLAM, MADHAVARAM MILK COLONY, CHENNAI-51

PHONE: 25557737, 25554288 FAX: 044-25559106,

E-MAIL: ascti.tnsc@gmail.com website: www.tnscbank.com

Accredited by: Centre for Professional Excellence in Co-operatives - (C-PEC) / BIRD, LUCKNOW

1. ருபே விவசாயக் கடன் அட்டை (Rupay Kisan Credit Card)

அறிமுகம்

விவசாயிகளுக்கு விரைவாகவும், எளிதாகவும் பயிர்க் கடன் மற்றும் சாகுபடி சார்ந்த செலவினங்களுக்கு கடன் கிடைக்கும் வண்ணம் விவசாயக் கடன் அட்டை திட்டத்தை 1998–99ஆம் ஆண்டில் மத்திய அரசு அறிமுகப்படுத்தியது. மேலும், வங்கிகள் மைய வங்கியியல் தீர்வு மற்றும் ஏடிஎம் வசதி, ஏடிஎம் டெபிட் கார்டு, ஆகிய வசதிகளை அறிமுகப்படுத்தியதுடன் விவசாயிகளும் நவீன வழியில் இத்திட்டத்தின் பயன்பாட்டினைக் கொண்டு விவசாயிகள் அவர்களுக்குத் தேவையான கடன் வசதிகளைப் பெறும் பொருட்டு, மத்திய அரசு ருபே விவசாயக் கடன் அட்டை திட்டத்தை 2012–13இல் அறிமுகப்படுத்தியது. ருபே விவசாயக் கடன் அட்டை என்பது இதர ஏடிஎம் கார்டுகள் போல் ஏடிஎம்கள் மூலம் விவசாயக் கடனின் பகுதியை ரொக்கமாக எடுக்கலாம், மற்றும் ருபே விவசாயக் கடன் அட்டைகளைக் கொண்டு அவர்கள் உரம் மற்றும் பூச்சி மருந்து ஆகியவைகளைக் கொள்முதல் செய்வதற்கு இக்கடன் அட்டைகளைப் பயன்படுத்திக் கொள்ளலாம்.

தொடக்க வேளாண்மைக் கூட்டுறவுக் கடன் சங்கங்கள் உறுப்பினர்களுக்கு பயிர்க் கடன்கள் வழங்கி வருகின்றன. பயிர்க் கடனில் ஒரு பகுதி வேளாண் இடுபொருட்களாகவும், மற்றொரு பகுதியான சாகுபடி செலவினம் ரொக்கமாகவும் வழங்கப்படுகிறது. தற்போது பணமில்லா பரிவர்த்தனைகளை ஊக்குவிக்கும் பொருட்டும், மேலும் பயிர்க் கடன் தொகையிலிருந்து விவசாயிகள் செலவிடும் சாகுபடி செலவினங்களை பணமில்லா பரிவர்த்தனைகள் மூலம் செலவிடுவதை ஊக்குவிக்கும் பொருட்டு இந்திய அரசு ருபே விவசாயக் கடன் அட்டை திட்டத்தை செயல்படுத்த தெரிவித்தது.

ருபே விவசாயக் கடன் அட்டைகள் வங்கிகளால் மட்டுமே வழங்க இயலும் என்பதால், தொடக்க வேளாண்மைக் கூட்டுறவுக் கடன் சங்கங்களில் பயிர்க் கடன் பெறும் விவசாயிகளுக்கு மத்தியக் கூட்டுறவு வங்கியில் சேமிப்புக் கணக்கு துவக்கி, மத்தியக் கூட்டுறவு வங்கிகள் தொடக்க வேளாண்மைக் கூட்டுறவு கடன் சங்க விவசாய உறுப்பினர்களுக்கு ருபே விவசாய கடன் அட்டை வழங்கப்படும். இந்தக் கணக்கில் பயிர்க் கடனின் ரொக்கப் பகுதி வரவு வைக்கப்படும்.

ருபே விவசாயக் கடன் அட்டையைக் கொண்டு இந்தியாவிலுள்ள எந்தவொரு ஏடிஎம் இயந்திரத்திலும், மைக்ரோ ஏடிஎம் இயந்திரத்திலும் பணப் பரிவர்த்தனைகளை மேற்கொள்ளலாம்.

செயலாக்கம்

நபார்டு வங்கி, தனது அலுவலக சுற்றறிக்கை எண் 248 நாள் 11.12.2014 வாயிலாக ருபே விவசாயக் கடன் அட்டை வழங்குவது சம்பந்தமான செயலாக்க மாதிரிகளை விளக்கியுள்ளது. இதில் நம் மாநிலத்தில் செயல்படுத்தப்படும் முறை குறித்துக் கீழே காண்போம்.

தமிழ்நாட்டில் ருபே விவசாயக் கடன் அட்டை வழங்குதல் குறித்த படிநிலைகள்

- தொடக்க வேளாண்மைக் கூட்டுறவுக் கடன் சங்க உறுப்பினர்களுக்கு மாவட்டமத்தியக் கூட்டுறவு வங்கியில் கேசிசி–சேமிப்புக் கணக்கு துவக்கப்பட வேண்டும். இக்கணக்கிற்கு மத்தியக் கூட்டுறவு வங்கியால் தொடக்க வேளாண்மைக் கூட்டுறவுக் கடன் சங்க உறுப்பினர்களுக்கு ருபே விவசாயக் கடன் அட்டைகட்டணம் ஏதுமின்றி வழங்கப்படும்.தனிப்பட்ட அடையாள எண் (PIN mailer) உறுப்பினரின் வீட்டிற்கு தபால்மூலம் அனுப்பி வைக்கப்படும்.கேசிசி–சேமிப்புக் கணக்கிற்கு குறைந்த பட்ச நிலுவைத் தொகை ஏதும் பராமரிக்கத் தேவையில்லை.
- ஒவ்வொரு தொடக்க வேளாண்மைக் கூட்டுறவுக் கடன் சங்கத்திற்கும் மாவட்ட மத்தியக் கூட்டுறவு வங்கியில் டிஜிட்டல் உறுப்பினர் பதிவேடு (Digital Member Register) பராமரிக்கப்பட வேண்டும். இப்பதிவேட்டில் தொடக்க வேளாண்மைக் கூட்டுறவுக் கடன் சங்க உறுப்பினர் வாரியாக நிலம் சம்பந்தப்பட்ட விவரங்கள், பயிர் விவரம், கடன் தொகை, ரொக்க அளவு, இடுபொருட்களுக்கான தொகை, போன்ற விவரங்கள் ஏற்றப்படும்.
- தொடக்க வேளாண்மைக் கூட்டுறவுக் கடன் சங்க உறுப்பினர்கள் பயிர்க் கடனுக்கான விண்ணப்பத்தினை சங்க செயலரிடம் அளிக்க வேண்டும்.
- உறுப்பினரின் விண்ணப்பம் பரிசீலிக்கப்பட்டு, கடனளவு நிர்ணயிக்கப்படும்.
- நிர்ணயிக்கப்பட்ட கடனளவு ரொக்கம் மற்றும் இடுபொருட்களுக்கான தொகை என இரண்டாகப் பிரிக்கப்படும்.
- இடுபொருட்களுக்கான பற்று எழுதப்பட்டு, இடுபொருட்கள் வழங்கப்படும்.
- மீதமுள்ள ரொக்கத் தொகையை உறுப்பினர் வாரியாக பட்டியலிட்டு, மத்தியக் கூட்டுறவு வங்கியின் கிளை மேலாளருக்கு காசோலையுடன் அனுப்பி வைக்கப்படும். காசோலை மற்றும் பட்டியல் பெற்ற மத்தியக் கூட்டுறவு வங்கிக் கிளை மேலாளரால், தொடக்க வேளாண்மைக் கூட்டுறவுக் கடன் சங்கத்தின் பயிர்க் கடன் காசுக் கடன் கணக்கில் பற்று வைத்து, பட்டியலில் குறிப்பிடப்பட்டுள்ள உறுப்பினர்களின் கேசிசி–சேமிப்புக் கணக்கில் வரவு வைக்கப்படும். வரவு வைக்கப்பட்ட விவரம், உறுப்பினர்களுக்கு கைபேசி வாயிலாக குறுந்தகவல் மூலம் அனுப்பி வைக்கப்படும்.

- குறுந்தகவல் செய்தி பெற்ற உறுப்பினர், இந்தியாவில் உள்ள எந்தவொரு ஏடிஎம் இயந்திரத்திலும் பணப் பரிவர்த்தனை மேற்கொள்ளலாம்.
- மேலும், தங்களுக்குத் தேவைப்படும் இடுபொருட்களுக்குத் தேவையான கட்டணத்தை ருபே விவசாயக் கடன் அட்டை மூலமாகச் செலுத்தலாம்.
- தொடக்க வேளாண்மைக் கூட்டுறவுக் கடன் சங்கங்கள் எப்பொழுதெல்லாம் உறுப்பினர்களக்கு கடனளவு நிர்ணயிக்கின்றதோ, அப்பொழுதெல்லாம் மத்தியக் கூட்டுறவு வங்கியில் உள்ள டிஜிட்டல் உறுப்பினர் பதிவேட்டில் கடனளவை உடனுக்குடன் பதிவேற்ற வேண்டும். இப்பதிவேற்றல் முறையை தொடக்க வேளாண்மைக் கூட்டுறவுக் கடன் சங்கங்கள் அதற்காக அளிக்கப்படும் இணையதளம் வாயிலாகவும் செய்ய முடியும்.
- உறுப்பினர், ஏடிஎம் இயந்திரத்திலோ அல்லது மின்னணு விற்பனைக் கருவி(PoS-Point of Sale) இயந்திரத்திலோ பணப் பரிவர்த்தனை மேற்கொள்ளும் போது உறுப்பினரின் கேசிசி–சேமிப்புக் கணக்கிலும், டிஜிட்டல் உறுப்பினர் பதிவேட்டில் உள்ள உறுப்பினர் கணக்கிலும் பற்று வைக்கப்படும்.
- உறுப்பினர்களின் பரிவர்த்தனைகள் மத்தியக் கூட்டுறவு வங்கியிலிருந்து தொடக்க வேளாண்மைக் கூட்டுறவுக் கடன் சங்கங்களுக்கு அனுப்பி வைக்கப்படும். இவ்விவரங்களை தொடக்க வேளாண்மைக் கூட்டுறவுக் கடன் சங்கங்கள் தங்களுடைய பதிவேடுகளிலும், கணினியிலும் பதிவேற்றம் செய்து கொள்ள வேண்டும்.
- ருபே விவசாயக் கடன் அட்டை பெற்ற உறுப்பினர்கள், தங்கள் அட்டையைப் பயன்படுத்தி வங்கியால் அனுப்பப்படும் தனிப்பட்ட அடையாள எண்ணை (PIN mailer) மாற்றம் செய்து கொள்ள அறிவுறுத்த வேண்டும்.
- உறுப்பினர்கள் பயிர்க் கடனைத் திருப்பிச் செலுத்தும்போது அதை தொடக்க வேளாண்மைக் கூட்டுறவுக் கடன் சங்கத்திலேயே செலுத்த வேண்டும். இப்பரிவர்த்தனைகளை Excel file வாயிலாக மத்தியக் கூட்டுறவு வங்கிக்கு அனுப்ப வேண்டும். மத்தியக் கூட்டுறவு வங்கி இப்பரிவர்த்தனைகளை டிஜிட்டல் உறுப்பினர் பதிவேட்டில் பதிவேற்றம் செய்யும்.
- உறுப்பினர்கள் இந்தியாவில் உள்ள எந்தவொரு ஏடிஎம் இயந்திரத்திலும் மாதம் ஒன்றுக்கு மெட்ரோ நகரங்களில் மூன்று முறை அல்லது பிற இடங்களில் ஐந்து முறை கட்டணமில்லாமல் பரிவர்த்தனைகளை மேற்கொள்ளலாம். அதற்கு மேல் பரிவர்த்தனைகள் மேற்கொள்ளும்பொழுது கட்டணம் செலுத்த வேண்டியிருக்கும்.

- மின்னணு விற்பனைக் கருவி(PoS-Point of Sale) இயந்திரத்திலோ அல்லது இணையவழியிலோ (Ecommerce) செய்யப்படும் பரிவர்த்தனைகளுக்கு எண்ணிக்கை கட்டுப்பாடு கிடையாது.

ருபே விவசாயக் கடன் அட்டை வழங்குதலில் தொடக்க வேளாண்மைக் கூட்டுறவுக் கடன் சங்கங்களின் பங்கு

1. உறுப்பினர்களின் கடன் விண்ணப்பத்தினைப் பரிசீலித்தல்
2. பரிசீலிக்கப்பட்ட விண்ணப்பத்தினை நிர்வாகக் குழுவிற்குச் சமர்ப்பித்தல்
3. கடன் வழங்குதல்
4. கடன் வசூலித்தல்
5. மத்தியக் கூட்டுறவு வங்கியின் டிஜிட்டல் உறுப்பினர் பதிவேட்டில் உடனுக்குடன் தரவினை ஏற்றுதல்

ருபே விவசாயக் கடன் அட்டையின் பயன்கள்

1. இக் கடன்அட்டைகள் எந்தவித கட்டணமும் இன்றி தொடக்க வேளாண்மைக் கூட்டுறவுக் கடன் சங்க உறுப்பினர்களுக்கு வழங்கப்படுகிறது.
2. இக் கடன் அட்டையைப் பயன்படுத்தி இந்தியா முழுவதிலுமள்ள எந்தவொரு ஏடிஎம் இயந்திரத்திலும் பணம் எடுக்கலாம். தங்களுடைய இடுபொருட்களுக்கான தொகையை PoS (Point of Sale) இயந்திரம் வாயிலாக ருபே விவசாயக் கடன் அட்டையை உபயோகப்படுத்தி செலுத்தலாம்.
3. பணப் பரிவர்த்தனை செலுத்தியவுடன் கைபேசிக்கு குறுந்தகவல் பெறலாம். அதனால், தங்கள் கணக்கில் உள்ள நிலுவைத் தொகையை உடனுக்குடன் அறிய முடியும்.
4. இனி வருங்காலங்களில், இக்கணக்கில் அரசின் மானியம், பயிர் காப்பீடு இழப்பீட்டுத் தொகை போன்ற அரசு சார் பணப் பரிவர்த்தனைகள் நடைபெறும்.
5. இதன் மூலம் மத்தியக் கூட்டுறவு வங்கிகள் அளிக்கும் அனைத்து வகையான நிதிச் சேவைகளையும் பெற முடியும்.
6. நாளுக்கு நாள் அதிகரித்து வரும் ரொக்கமில்லா பணப் பரிவர்த்தனைகளை தொடக்க வேளாண்மைக் கூட்டுறவுக் கடன் சங்க உறுப்பினர்களும் செய்ய முடியும்.

ரூபே விவசாயக் கடன் அட்டை உறுப்பினருக்கான விபத்துக் காப்பீட்டுத் திட்டம்

ரூபே விவசாயக் கடன் அட்டை வைத்திருப்போருக்கு இந்திய தேசிய பரிவர்த்தனை நிறுவனத்தால் (National Payments Corporation of India) விபத்துக் காப்பீடு அளிக்கப்படுகிறது. இத்திட்டத்தின் விவரங்கள் கீழே கொடுக்கப்பட்டுள்ளன.

திட்ட விவரங்கள்

- உறுப்பினர்,விபத்து ஏற்பட்டு உயிரிழந்தாலோ அல்லது விபத்தில் நிரந்தர உடல் ஊனமுற்றாலோ காப்பீட்டுத் தொகை ரூ.1 இலட்சம் வரை வழங்கப்படும்.
- இத்திட்டம் 1.4.2017 முதல் 31.3.2018 வரை நடைமுறையில் இருக்கும். இந்திய தேசிய பரிவர்த்தனை நிறுவனத்தால் இத்திட்டம் மேலும் நீட்டிக்கப்படலாம்.
- மத்திய அரசின் இன்சூரன்ஸ் நிறுவனமான New India Assurance Company நிறுவனத்தின் வாயிலாக இத்திட்டம் செயல்படுத்தப்படுகிறது.
- இத்திட்டத்தின் மூலம் உறுப்பினர் பயன் அடையவேண்டுமானால், விபத்து நடைபெற்ற நாளிலிருந்து 90 நாட்கள் முன்னதாகக் குறைந்தபட்சம் ஒரு முறையாவது ரூபே விவசாயக் கடன் அட்டையை, ஏதாவதொரு ஏடிஎம் இயந்திரத்திலோ அல்லது PoS (Point of Sale) இயந்திரத்திலோ உபயோகப்படுத்தி இருக்க வேண்டும்.
- விபத்து நடைபெற்ற நாளிலிருந்து 90 நாட்களுக்குள் காப்பீட்டுத் தொகை கோரிக்கை விண்ணப்பத்தினை (Claim Form)மத்தியக் கூட்டுறவு வங்கி வாயிலாக இன்சூரன்ஸ் நிறுவனத்திற்கு அளிக்க வேண்டும்.

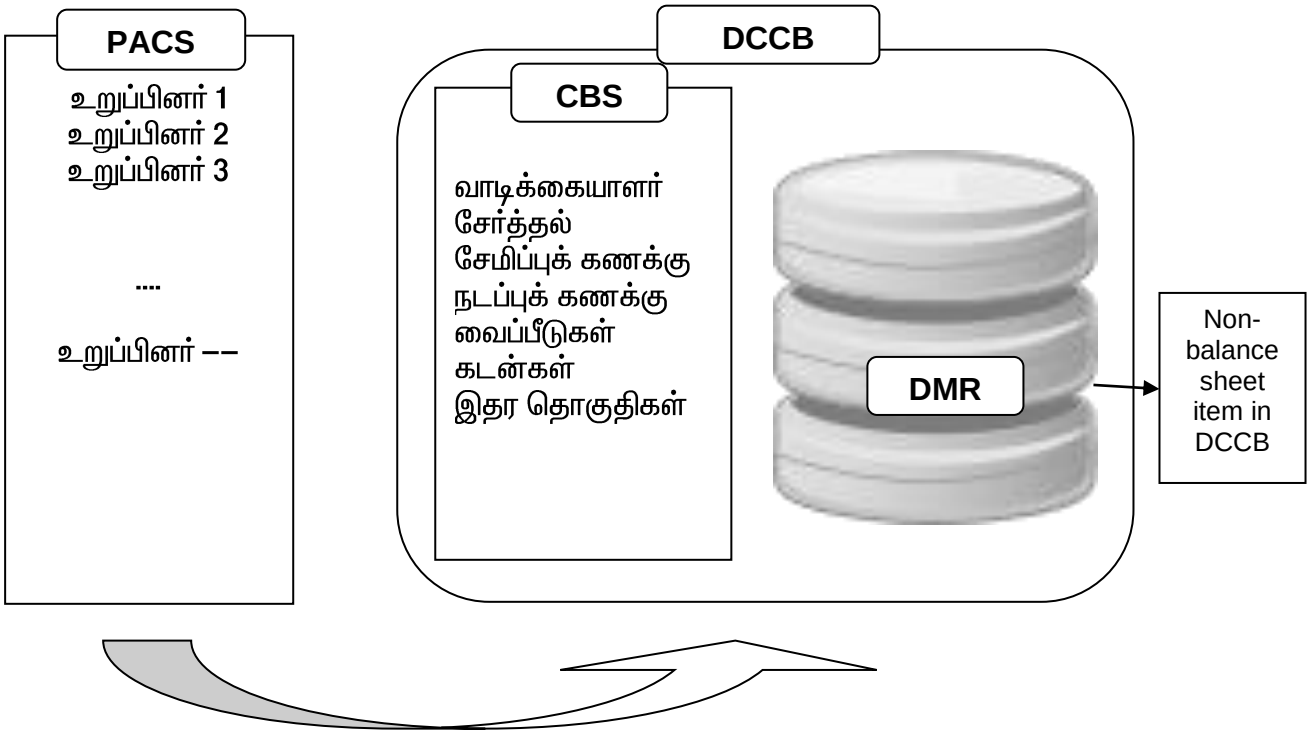
இத்திட்டம் குறித்து மேலும் தகவல் தேவைப்படின் மத்தியக் கூட்டுறவு வங்கியின் கிளைகளை அணுகவும்.

2. டிஜிட்டல் உறுப்பினர் பதிவேடு

Step 1

மத்தியக் கூட்டுறவு வங்கியில் டிஜிட்டல் உறுப்பினர் பதிவேடு (Digital Member Register-DMR) உருவாக்கம்

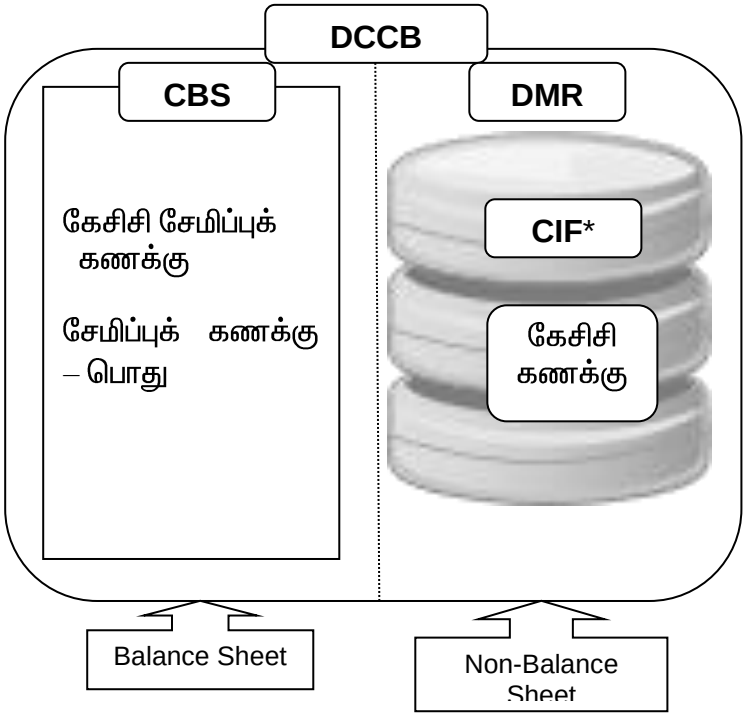
1. மத்தியக் கூட்டுறவு வங்கி CBS மென்பொருளில் சங்க வாடிக்கையாளர்களுக்கு சிறப்பு வாடிக்கையாளர் வகை (customer type) உருவாக்குதல்
2. சங்க வாடிக்கையாளர்களின் சேமிப்புக் கணக்கிற்கு சிறப்பு கணக்கு வகை (product type) உருவாக்குதல்
3. டிஜிட்டல் உறுப்பினர் பதிவேட்டில் சங்க உறுப்பினர்களுக்கு கேசிசி கணக்கு (product) உருவாக்குதல்



Step 2

டிஜிட்டல் உறுப்பினர் பதிவேட்டில் தரவு உருவாக்குதல் / ஏற்றுதல் (DMR Data creation / loading)

1. சங்க உறுப்பினர்களின் KYC தகவல்கள் சரிபார்க்கப்பட்டபின் மத்தியக் கூட்டுறவு வங்கியில் கணக்கு துவக்கப்படும்.
2. விவசாயிகளின் KCC கணக்கு DMRல் துவக்கப்படும்.
3. விவசாயிகளின் DMR கணக்கிற்கும், தொ.வே.கூ.க. சங்கங்கள் மத்தியக் கூட்டுறவு வங்கியிலுள்ள சேமிப்புக் கணக்கிற்கும் இணைப்பு ஏற்படுத்துதல்.



* Customer Information file

Step 3

உறுப்பினர் கடனைத் திருப்பிச் செலுத்தும்போது டிஜிட்டல் உறுப்பினர் பதிவேட்டில் தரவினை மேம்படுத்துதல் (DMR data updation)

1. மத்தியக் கூட்டுறவு வங்கியின் CBS வாயிலாக DMR கணக்கினைப் பார்க்க முடியும்.
2. சங்க உறுப்பினர்களின் கணக்கு, மத்தியக் கூட்டுறவு வங்கியின் CBS மற்றும் DMRல் வரவு செலவு செய்யப்படும்.
3. தொடக்க வேளாண்மைக் கூட்டுறவுக் கடன் சங்கங்கள், தாங்கள் வைத்துள்ள உறுப்பினர் கடன் கணக்கில் நடக்கும் வரவு செலவினை மத்தியக் கூட்டுறவு வங்கியில் உள்ள DMR கணக்கிற்கு ஃபைல் வாயிலாக பதிவேற்றம் செய்யலாம்.
4. அதேபோல், மத்தியக் கூட்டுறவு வங்கியில் உறுப்பினர்களின் கணக்கில் நடக்கும் வரவு செலவினை ஃபைல் வாயிலாக பதிவிறக்கம் செய்யலாம்.

ருபே விவசாயக் கடன் அட்டை பரிவர்த்தனை ஓட்டம்
(RUPAY KCC TRANSACTION FLOW)

ஏடிஎம் ஸ்விட்ச்

DCCB

CBS

DMR

கேசிசி சேமிப்புக் கணக்கு

சேமிப்புக் கணக்கு – பொது

உறுப்பினரின் கேசிசி கணக்கு – ரொக்க வரம்பு

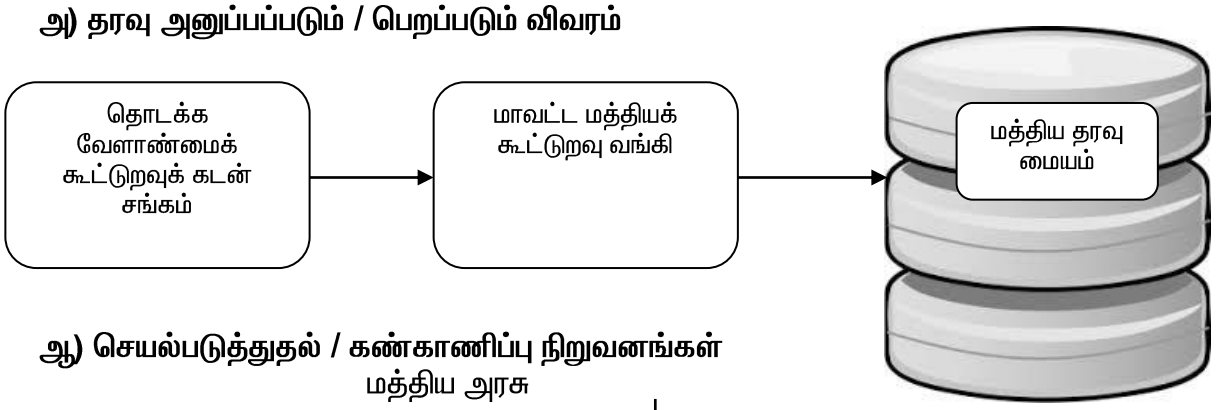
கடன் 1

கடன் 2

கடன் 3

3) தொடக்க வேளாண்மைக் கூட்டுறவுக் கடன் சங்கங்களில் நடைமுறைப்படுத்தப்பட உள்ள மைய வங்கியியல் தீர்வுக்கான கட்டமைப்பு (CBS Architecture)

அ) தரவு அனுப்பப்படும் / பெறப்படும் விவரம்



ஆ) செயல்படுத்துதல் / கண்காணிப்பு நிறுவனங்கள்

மத்திய அரசு

↓

நபார்டு வங்கி

↓

மாநில அரசு

↓

தலைமைக் கூட்டுறவு வங்கி

↓

மாவட்ட மத்தியக் கூட்டுறவு வங்கி

↓

தொடக்க வேளாண்மைக் கூட்டுறவுக் கடன் சங்கம்

இ) மென்பொருள் நிறுவனங்கள்

தேசிய தொடக்க வேளாண்மைக் கூட்டுறவுக் கடன் சங்க மென்பொருள் நிறுவனம் (National Level PACS Software Vendor – NLPSV)

தேசியதரவு களஞ்சிய நிறுவனம் (National Level Data Repository Vendor – NLDRV)

↓

ஒருங்கிணைப்பாளர் (System Integrator – SI)

Role:

- வன்பொருள் வழங்கல்/நிறுவுதல்
- மென்பொருள் நிறுவுதல்
- பணியாளர்களுக்கு பயிற்சி அளித்தல்
- தரவு மேலாண்மை (data digitization and migration)

↓

தொடக்க வேளாண்மைக் கூட்டுறவுக் கடன் சங்கம்

4. TNSC வங்கியின் வலையவங்கிச் சேவை (RETAIL NET BANKING)

தொடக்கவேளாண்மைக் கூட்டுறவுக் கடன் சங்கங்களுக்குபயன்பாட்டுச் சேவைகள் (Utility Bill Payments) வழிகாட்டி

தலைமைக் கூட்டுறவு வங்கி, தொடக்கவேளாண்மைக் கூட்டுறவுக் கடன் சங்கங்களுக்குபயன்பாட்டுச் சேவைகளை (Bill Payments facilities) வழங்கி வருகிறது.

கணக்குஇயக்கும் வழிமுறைகள்

- ஒவ்வொருதொடக்கவேளாண்மைக் கூட்டுறவுக் கடன் சங்கத்திற்கும் இச்சேவைக்கென ஒருநடப்புக் கணக்குதலைமை வங்கியில்தொடங்கவேண்டும். (பயன்பாட்டுச் சேவைக் கணக்கு)
- சங்கப் பணியாளர் ஒருவருக்குநடப்புக் கணக்கினை வலைய வங்கியியல் மூலமாகஇயக்கஅதிகாரம் வழங்கி நிர்வாகக் குழு தீர்மானம் நிறைவேற்றவேண்டும்.
- கணக்கைஇயக்கும் அதிகாரம் பெற்றவருக்குகடவுச் சொல் (password) வழங்கப்படும். இதனைக் கொண்டு பயன்பாட்டுச் சேவைக் கணக்கின் மூலம் இச்சேவையை வாடிக்கையாளருக்கு வழங்க இயலும்.
- கடவுச் சொல்லைப் பயன்படுத்தித்தான் பயன்பாட்டுச் சேவைக் கணக்கினை இயக்கமுடியும். எனவே பணப்பரிவர்த்தனைகள்அனைத்தும் கடவுச் சொல் மூலமேநடைபெறும். எனவே, வலைய வங்கியியல் மூலம் நடைபெறும் பணப்பரிவர்த்தனைகளுக்குதொடக்கவேளாண்மைக் கூட்டுறவுக் கடன் சங்கம் மட்டுமேபொறுப்பாகும்.
- தமிழ்நாடுமாநிலத் தலைமைக் கூட்டுறவு வங்கி, இச்சேவையைவழங்கும் வசதியைஏற்படுத்தித் தருபவர் மட்டுமே. எனவே, தமிழ்நாடுமாநிலத் தலைமைக் கூட்டுறவு வங்கிக்கு எந்தவிதபணச் சுமையோமற்றும் நிதிப் பொறுப்போதொடக்கவேளாண்மைக் கூட்டுறவுக் கடன் சங்கங்கள்வலைய வங்கியியல் மூலம் மேற்கொள்ளும் பணப்பரிவர்த்தனைகளுக்கு கிடையாதுஎன்பதனைதெளிவாகப் புரிந்துகொள்ளவேண்டும். (No financial responsibility and no financial liability for TNSC Bank)
- தமிழ்நாடுமாநிலத் தலைமைக் கூட்டுறவு வங்கிக்கு Bill Desk வணிகக் கூட்டாளர் (Aggregator) வழங்கும் எல்லாசேவைகளும் தொடக்கவேளாண்மைக் கூட்டுறவுக் கடன் சங்கங்களுக்கும் வழங்கப்படும்.

பயன்பாட்டுச் சேவைகணக்கிற்கு பணம் செலுத்தும் முறை

- பயன்பாட்டுச் சேவைநடப்புக் கணக்கிற்குத் தேவையான பணத்தை தொடக்க வேளாண்மைக் கூட்டுறவுக் கடன் சங்கம் NEFT மூலம் மத்தியக் கூட்டுறவு வங்கி வழியாகமாற்றம் செய்யவேண்டும்.
- பயன்பாட்டுச் சேவைநடப்புக் கணக்கில் ரொக்கஇருப்பு இருக்கும் பட்சத்தில்மட்டுமேவாடிக்கையாளர்களுக்குச் சேவைவழங்கஇயலும் என்பதால், இந்நடப்புக் கணக்கில் போதியரொக்கஇருப்பைதொடக்கவேளாண்மைக் கூட்டுறவுக் கடன் சங்கங்கள்பராமரிக்கவேண்டும்.

நிர்வாகக் குழு மற்றும் பணியாளர்களின் முக்கியபொறுப்பு

1. இச்சேவைநடப்புக் கணக்கில் நடைபெறும் அனைத்துபணப் பரிவர்த்தனைகளுக்கும் தொடக்கவேளாண்மைக் கூட்டுறவுக் கடன் சங்கங்கள்பொறுப்பாகும்.
2. பணியாளர்கள் ஓய்வு பெறும்போது, தமிழ்நாடுமாநிலத் தலைமைக் கூட்டுறவு வங்கிக்கு, அப்பணியாளரின் யூசர் ஐ.டி. (User id), கடவுச் சொல்லைநிறுத்தம் செய்யதெரிவிக்கவேண்டும். அப்பணிக்குவேறுபணியாளரைநிர்வாகக் குழுவின் தீர்மானம் மூலம் நியமனம் செய்யவேண்டும். புதியபணியாளர்களுக்குபுதியயூசர் ஐ.டி. மற்றும் கடவுச் சொல்லைப் பெற்றுக் கொள்ளவேண்டும். இதற்குச் தொடக்கவேளாண்மைக் கூட்டுறவுச் கடன் சங்கமும், நிர்வாகக் குழுவுமே முழு பொறுப்பாகும்.
3. பணியாளர் பணியில்இடைநீக்கம் செய்யப்பட்டாலோஅல்லதுநீண்டவிடுமுறையில்செல்ல நேர்ந்தாலோ, தமிழ்நாடுமாநிலத் தலைமைக் கூட்டுறவு வங்கிக்கு, அப்பணியாளரின் யூசர் ஐ.டி., கடவுச் சொல்லைநிறுத்தம் செய்யதெரிவிக்கவேண்டும். அப்பணிக்குவேறுபணியாளரைநிர்வாகக் குழுவின் தீர்மானம் மூலம் நியமனம் செய்யவேண்டும். புதியபணியாளர்களுக்குபுதியயூசர் ஐ.டி. மற்றும் கடவுச் சொல்லைப் பெற்றுக் கொள்ளவேண்டும். இதற்குச் சங்கம் மற்றும் நிர்வாகக் குழு முழு பொறுப்பாகும்.
4. தமிழ்நாடுமாநிலத் தலைமைக் கூட்டுறவு வங்கி வழங்கும் வலைய வங்கியியல்விதிமுறைகள்மாறும் போது, அம்மாற்றம் தொடக்கவேளாண்மைக் கூட்டுறவுக் கடன் சங்கங்களின் தனிநபர் வலைய வங்கியியல்சேவைக்கும் பொருந்தும்.

கடவுச் சொல்பாதுகாப்பு

1. கடவுச் சொல்என்பதுதொடக்கவேளாண்மைக் கூட்டுறவுக் கடன் சங்கத்தின் தீர்மானத்தின்படிவழங்கப்படுகிறது. எனவேபயன்பாட்டுக் கணக்கினை இயக்குபவர் கடவுச் சொல்லைப் பாதுகாப்பாகவைத்திருக்கவேண்டும்.
2. கடவுச் சொல்லைஎங்கும் எழுதிவைக்கக் கூடாது. அதனைநினைவில்நிறுத்திக் கொள்ளவேண்டும்.
3. கடவுச் சொல்லைமறந்தால்அதனைவலைய வங்கியியலின் மூலம் மாற்றிக் கொள்ளலாம்.
4. கடவுச் சொல்லைஅடிக்கடிமாற்றம் செய்யவேண்டும். இதன் மூலம் கடவுச் சொல்பாதுகாப்புபெறுகிறதுஎன்பதைத் தெரிந்துகொள்ளவும்.
5. கடவுச் சொல் 90 நாட்களுக்குமட்டுமேசெல்லுபடியாகும். எனவே, 90 நாட்களுக்குஒருமுறைகட்டாயமாககடவுச் சொல்லைமாற்றம் செய்யவேண்டும்.
6. கடவுச் சொல்என்பதனைஇரகசியமாகவைத்துக் கொள்ளவேண்டும். கடவுச் சொல்லையாருடனும் பகிர்ந்து கொள்ளக் கூடாது.
7. தொடக்கவேளாண்மைக் கூட்டுறவுக் கடன் சங்கத்தின் பயன்பாட்டுக் கணக்கினை நாள்தோறும் முறைப்படி நேர் செய்யவேண்டும்.
8. சங்கம் www.tnscbank.netஎன்றஇணையதளத்தில்Log செய்து (மெனு–Account -> Statement of Accounts) நடப்புக் கணக்குபரிவர்த்தனைகளைசரிபார்த்து நாள்தோறும் PDF அச்சுப் பிரதிஎடுத்துகோப்பில்வைக்கவேண்டும்.

நடப்புக் கணக்கு பரிவர்த்தனையை சரிபார்க்க மற்றும் கணக்கு அறிக்கையை அச்சுப் பிரதிஎடுத்தல் குறித்த விவரம்

சங்கப் பணியாளர் / அனுமதிக்கப்பட்ட பணியாளர் www.tnscbank.net என்ற இணையதளத்தில் log-in செய்து, வலைய வங்கியியல்யூசர் ஐ.டி. மற்றும் கடவுச் சொல்லைஉபயோகித்து, ஒவ்வொருதேதிக்கும் வலைய வங்கியியல் மூலம் மேற்கொண்ட பரிவர்த்தனை பணிகளின் விவரங்களை கீழ்க்கண்டவாறு பதிவிறக்கம் செய்து, தனியாக பதிவேட்டில் ஒட்டிவைக்கவேண்டும். இந்தப் பரிவர்த்தனை விவரங்கள் சங்க கணக்குகளில் வரவு செலவு செய்ய ஆதாரமாக இருக்கும்.

Log In ⟶ Menu ⟶ Accounts ⟶ Statement of Accounts ⟶ select 'A/c. No.' ⟶
Give 'From Date' & 'To Date' ⟶Format Type ⟶ Select 'PDF' ⟶ Click 'Download' ⟶
Save on Desktop ⟶ Take Print

- இந்தக் கணக்கு அறிக்கையில் (Statement of Accounts)சங்கம் அன்றைய தேதியில் மேற்கொண்ட வரவு செலவுகள்அனைத்தும் இடம் பெறும்.
- இதனை, சங்கம் அன்றைய தேதிய பற்றுச் சீட்டுடன் (Vouchers) ஒப்பிட்டு சரிபார்த்துக் கொள்ள வேண்டும்.
- கணக்கு அறிக்கையை (PDF) அச்சுப் பிரதி எடுத்து தணிக்கைக்காக கோப்பில் சேர்க்க வேண்டும்.
- மேற்கண்டவாறு பதிவிறக்கம் செய்து தனியாக பதிவேட்டில் பராமரித்து, சங்க கணக்குகளில் வரவு செலவு செய்வதை ஆய்வு அலுவலர்கள் உறுதி செய்து கொள்ள வேண்டும்.

5) ஆதார் மூலம் பணப் பரிவர்த்தனைசேவை
(Aadhaar Enabled Payment System - AEPS)

ஆதார் எண்ணைக் கொண்டு வங்கி சார்ந்த பணப் பரிவர்த்தனைகளைமேற்கொள்ளும் சேவையேAEPSஎனும் சேவையாகும்.மைக்ரோஏடிஎம் மற்றும் மின்னணுவிற்பனைக் கருவி(PoS-Point of Sale)வாயிலாககீழ்க்கண்டசேவைகளைவாடிக்கையாளர் பெறமுடியும்.

1. இருப்புவிசாரணை (Balance Enquiry)
2. பணம் எடுத்தல் (Cash withdrawal)
3. பணம் செலுத்துதல் (Cash deposit)
4. ஒரு ஆதார் எண்ணிலிருந்துமற்றொருஆதார் எண்ணிற்குபணப் பரிவர்த்தனை (Aadhaar to Aadhaar Fund Transfer)

இச்சேவையைப் பெறுவதற்குவாடிக்கையாளர் தங்கள்கணக்கில் ஆதார் எண்ணை இணைத்திருக்க வேண்டும்.

வருங்காலத்தில்ஒவ்வொருதொடக்கவேளாண்மைக் கூட்டுறவுக் கடன் சங்கத்திற்கும் மைக்ரோஏடிஎம் அல்லதுமின்னணுவிற்பனைக் கருவி(PoS-Point of Sale)அளிக்கப்படும். சங்கங்கள், தங்களுடைய வாடிக்கையாளர்களுக்கு மட்டுமல்லாமல் இதர வங்கி வாடிக்கையாளர்களுக்கும் மேற்கூறிய சேவைகளை வழங்கமுடியும். இதனால் அச்சங்கங்கள் இதர வங்கிகளிடமிருந்து சேவைக் கட்டணம் பெற்று, தங்களுடைய நிதியாதாரத்தை மேம்படுத்தமுடியும்.

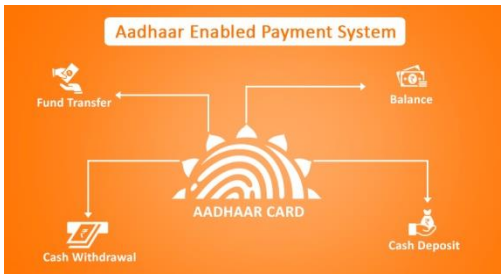
இச் சேவையைஉபயோகப்படுத்தி, சங்கஉறுப்பினர்கள்தங்களுடையருபேவிவசாயக் கடன் அட்டையைஉபயோகப்படுத்திபணப் பரிவர்த்தனைகளைமேற்கொள்ளலாம்.

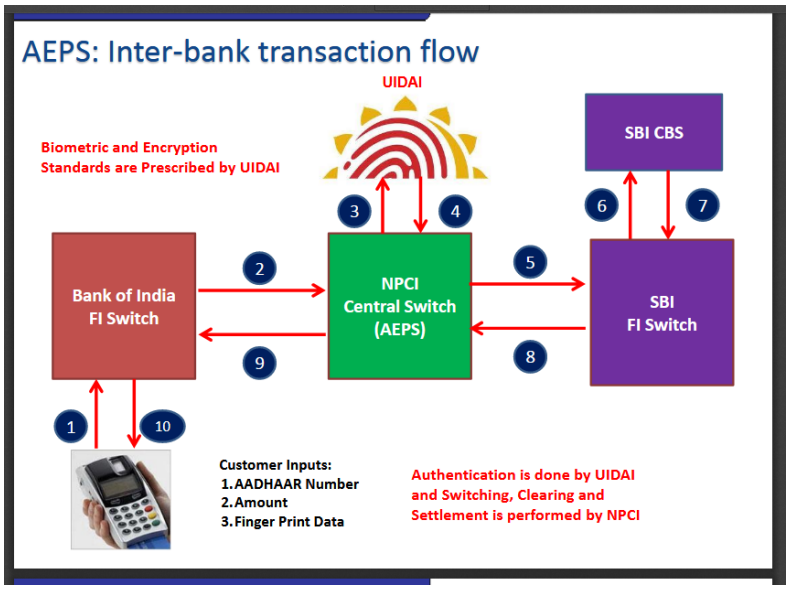
இச்சேவைசெயல்படும் விதம்

1. வாடிக்கையாளர் தங்களுடைய வங்கிக் கணக்கில் ஆதார் எண்ணை இணைக்க வேண்டும்.
2. இச்சேவை அளிக்கும் வங்கிக் கிளையிலோ, வணிக முகவர்களிடமோ (Business Correspondents) சென்று, தங்களுடைய ஆதார் எண்ணையும், வங்கி விவரங்களையும் தெரிவிக்கவேண்டும்.
3. பின்னர், தங்களுடைய விரல் ரேகையைப் பதிய வேண்டும்.

4. இவ்விரல்ரேகை, ஆதார் அட்டைவழங்கிய இந்தியதனித்துவஅடையாளஆணையத்தின் (Unique Identification Authority of India) கணினியில்ஏற்கனவேஉள்ளரேகையுடன் ஒப்பிட்டுப் பார்க்கப்படும்.
5. இரண்டுரேகைகளும் சரியாக இருப்பின், வாடிக்கையாளர் தங்களுடையகணக்கைக் கொண்டுமேற்கூறியநான்குவிதமானசேவைகளைப் பெறலாம்.

இச்சேவையைப் பற்றிய தொழில்நுட்பவிளக்கம் கீழேகொடுக்கப்பட்டுள்ளது.





மைக்ரோ ஏடிஎம் இயந்திரம்

ஏடிஎம் இயந்திரத்தின் சிறிய பதிப்பே மைக்ரோ ஏடிஎம். மைக்ரோ ஏடிஎம் இயந்திரம் ஜிபிஆர்எஸ் வாயிலாக வங்கியுடன் இணைக்கப் பட்டிருக்கும். இதன் மூலம் வங்கிச் சேவைகளை எந்தவொரு இடத்திலும், எந்தவொரு நேரத்திலும் வாடிக்கையாளர்களுக்கு அளிக்கமுடியும்.

இந்த இயந்திரத்தின் வாயிலாக டெபிட் கார்டு, கிரடிட் கார்டு மற்றும் ஆதார் எண் மூலமாக கீழ்க்காணும் வங்கிச் சேவைகளை வாடிக்கையாளர்குலூ பெறமுடியும்.

மைக்ரோஏடிஎம் இயந்திரத்தின் மூலம் மேற்கொள்ளப்படும் வங்கிச் சேவைகள்

1. பணம் டெபாசிட் செய்தல்
2. பணம் எடுத்தல்
3. பணம் அனுப்புதல்
4. பணம் கையிருப்புவிசாரணை
5. இ–கேஒய்சிவாயிலாகசேமிப்புக் கணக்குதுவக்கம்

மைக்ரோஏடிஎம் இயந்திரம் எப்படிஇயங்குகிறது ?

1. வாடிக்கையாளரின் டெபிட் கார்டு அல்லது கிரடிட் கார்டை மைக்ரோ ஏடிஎம் இயந்திரத்தில் தேய்க்க வேண்டும். அல்லது ஆதார் அட்டை உடன் கைரேகையை அழுத்த வேண்டும். இதன் மூலம் வாடிக்கையாளர் சரிபார்ப்பு நடைபெறும்.
2. சரிபார்ப்பு முடிந்தவுடன், வாடிக்கையாளருக்குத் தேவைப்படும் பரிவர்த்தனைகளை இந்த இயந்திரம் காண்பிக்கும்.
3. வாடிக்கையாளருக்குத் தேவைப்படும் பரிவர்த்தனை விருப்பத்தைத் தேர்வு செய்தபின்னர், அதற்கானபரிவர்த்தனை நடைபெறும்.
4. பரிவர்த்தனை வெற்றிகரமாக முடிந்த பின், மைக்ரோ ஏடிஎம் இயந்திரத்தில் அதற்குண்டான தகவல் அந்த இயந்திரத்திலுள்ள திரையில் காட்டப்படும். ஆதற்கான இரசீது உடனுக்குடன் அச்சடித்து வாடிக்கையாளர்க்குத் தரப்படும்.
5. பரிவர்த்தனை நிறைவு பெற்ற பின்னர், வங்கியிலிருந்து வாடிக்கையாளர்களுக்கு குறுந்தகவல் செய்தி அனுப்பப்படும்.

தொடக்கவேளாண்மைக் கூட்டுறவுக் கடன் சங்கங்களில்மைக்ரோஏடிஎம் நிறுவுவதால்ஏற்படும் நன்மைகள்

1. ருபேவிவசாயக் கடன் அட்டைவாயிலாக பணம் எடுக்க விரும்பும் உறுப்பினர்களுக்கு சங்க அளவிலேயே பணம் அளிக்கலாம். இதற்கான பரிவர்த்தனை மத்தியக் கூட்டுறவு வங்கியில் நடைபெறும்.

2. இந்த இயந்திரத்தைப் பயன்படுத்தி எந்தவொரு இடத்திலும் வங்கிச் சேவைகளைஅளிக்கமுடியும்.

3. இச்சேவைஅளிப்பதால்சங்கங்களுக்குவருவாய் கிடைக்கும்.

4. பயோமெட்ரிக் முறையும் இருப்பதால் வாடிக்கையாளரின் ஆதார் எண் மற்றும் கைரேகையைப் பயன்படுத்தி வங்கிச் சேவை அளிக்கும்போது பாதுகாப்பானதாக இருக்கும்.
5. கிராமபுறப் பகுதிகளில் அரசின் டிஜிட்டல் நிதி பரிவர்த்தனைகளை ஊக்குவிக்க இயலும்.

6. தமிழ்நாடு அரசின் முதியோர் ஓய்வூதியத் திட்டம் (Old age pension) தொடக்க வேளாண்மைக் கூட்டுறவுக் கடன் சங்கங்களின் வாயிலாக அளிக்க முடியும்.

7. எந்தவொரு ஏடிஎம் டெபிட் கார்டையும் பயன்படுத்தி இதன் மூலம் பணப் பரிவர்த்தனை செய்யலாம்.

6) இலக்கவங்கியியல்
(DIGITAL BANKING)

மின்னணு வங்கியியல் என்பது காலம் தொட்டு நடைமுறையில் இருக்கும் பணப்பரிமாற்றம், காசோலை வழங்குதல் மற்றும் அனைத்து வங்கிச் சேவைகளையும் வாடிக்கையாளர்களுக்கு கணினி மூலம் வழங்குதல் ஆகும். நமது நாட்டில் 1980–க்கு முன்பு அனைத்து வங்கிப் பணிகளும் கைமுறை செயல்பாட்டின் மூலமே நடைபெற்றது. வங்கிக் கணக்கினை பதிவதற்கு பேரேடு(Ledger)மற்றும் புத்தகம்(Register)ஆகியவை பயன்படுத்தப்பட்டது.

ஆகையால் ஒரு வாடிக்கையாளர் அவரது வங்கிக் கிளைக்குள் சென்றதும் அவருடைய கணக்கு எண் பராமரிக்கப்படும் பேரேடு எந்த கவுண்ட்டரில் உள்ளதோ அந்தக் கவுண்ட்டருக்கு சென்று அவரது பணப் பரிவர்த்தனைகளை செய்யத் தொடங்க வேண்டும், இதன் காரணமாக சில கவுண்ட்டர்களில் சில சமயங்களில் வாடிக்கையாளர்களே இல்லாமலும், சில கவுண்ட்டர்களில் வாடிக்கையாளர்கள் நீண்ட வரிசையில் நின்று பணப் பரிவர்த்தனை செய்யக் கூடிய சூழ்நிலை இருந்தது. இக்கால கட்டத்தில் வங்கி வாடிக்கையாளர் ஒவ்வொருவரும் பணப் பரிமாற்றத்திற்கு பல மணி நேரம் வங்கி கவுண்ட்டரில் செலவழிக்கும் நிலையே இருந்தது.

இந்திய ரிசர்வ் வங்கி, வங்கிகளில் வாடிக்கையாளர் சேவையை மேம்படுத்துவதற்காக பல குழுக்களை அமைத்தது. அக்குழுக்கள் வங்கிகளை கணினிமயமாக்குவதன் மூலம் பரிவர்த்தனை நேரத்தைக் குறைக்க முடியும் என்றும் அதனால் வாடிக்கையாளர் சேவையை மேம்படுத்த முடியும் என்றும் பரிந்துரைத்தன. இதன் தொடர்ச்சியாக 1990–ம் ஆண்டுக்குப் பிறகு பல வங்கிகள் படிப்படியாகக் கணினிமயமாக்கப்பட்டன.

முழுக்கிளை தானியக்கம்

(TOTAL BRANCH AUTOMATION - TBA)

கைமுறை செயல்பாடுகளில் உள்ள குறைகளை நிவர்த்தி செய்வதற்காக கிளையின் அனைத்து செயல்பாடுகளையும் கணினிமயமாக்கும் முறை செயல்படுத்தப்பட்டது. அதாவது ஒவ்வொரு கிளையில் உள்ள அனைத்து வாடிக்கையாளர்களின் கணக்கு விவரங்களும் அந்தக் கிளையிலேயே வைக்கப்பட்டிருக்கும் கணினி சர்வரில் உள்ள தரவுத் தளத்தில் (DATA BASE) சேமித்து வைக்கப்பட்டன. அந்தக் கிளையில் உள்ள அனைத்து கணினிகளும் இந்த சர்வருடன் நெட் வொர்க் மூலம் இணைக்கப்பட்டன. இதன் மூலம் வங்கி ஊழியர் எந்த கவுண்ட்டரில் இருந்தாலும் எல்லா வாடிக்கையாளர் கணக்கு எண்ணையும் அணுக (ACCESS) முடியும்.எனவே வங்கி வாடிக்கையாளர் எந்த கவுண்ட்டரில் வேண்டுமானாலும் பணப் பரிவர்த்தனை செய்ய முடியும். இந்த கணினிமயமாக்கல் முறை முழுக்கிளை தானியக்கம் (TOTAL BRANCH AUTOMATION – TBA) என்று அழைக்கப்பட்டது.

தரவு பிரித்தெடுத்தல் (DATA EXTRACTION)

முழுக்கிளை தானியக்கம் செய்வதற்கு பேரேடுகளில் உள்ள மூலத் தரவுகளை பிரித்தெடுத்து கணினியில் சேமிக்க வேண்டும். இதற்காக மூலத்தரவுகளை அதற்காக பிரத்யேகமாக தயாரிக்கப்பட்டிருக்கும் MS-EXCEL போன்ற விரிவுத்தாள்களில் சேமிக்க வேண்டும். இதுவே தரவு பிரித்தெடுத்தல் (DATA EXTRACTION) என்று அழைக்கப்படுகிறது.

தரவு செல்லுபடியாக்கல் (DATA VALIDATION)

பிரித்தெடுக்கப்பட்டுMS-EXCEL போன்ற விரிவுத்தாள்களில் சேமித்து வைத்திருக்கக்கூடிய தரவுகளை அதற்காக பிரத்யேகமாக தயாரிக்கப்பட்டிருக்கும் மென்பொருள் மூலம் சரிபார்க்கும் முறைக்கு தரவு செல்லுபடியாக்கல் (DATA VALIDATION) என்று பெயர்.

தரவு இடம் பெயர்வு (DATA MIGRATION)

தரவு இடம் பெயர்வு (DATA MIGRATION) என்பது செல்லுபடியாக்கப்பட்ட தரவுகளை அதற்கான மென்பொருள் கருவி (SOFTWARE TOOL) கொண்டு நாம் உபயோகப்படுத்தும் பயன்பாட்டு மென்பொருளில் கொண்டு சென்று சேமிக்கும் முறை ஆகும்.

இவ்வாறு மாற்றப்பட்ட கணக்கு விபரங்கள் சரியாக மாற்றப்பட்டுள்ளனவா என்று வங்கி ஊழியர்களால் சரி பார்க்கப்பட வேண்டும்.

கணினி தணிக்கை (SYSTEM AUDIT)

கணினிமயமாக்கப்படும்போது மூலத் தரவுகள் எவ்வித மாறுதலுமின்றி பயன்பாட்டு மென்பொருளில் சேமிக்கப்பட்டுள்ளதா என்பதையும் அவ்வாறு சேமிக்கப்பட்டபின் பயன்பாட்டு மென்பொருள் சரியாக இயங்குகிறதா என்பதையும் பல வழிகளில் சோதனை செய்ய வேண்டியது மிகவும் அவசியமாகும். இதற்காக டேட்டா மைக்கிரேஷன் செய்யப்பட்ட பிறகு பயன்பாட்டு மென்பொருள் சரியாக செயல்படுகிறதா என்பதை தணிக்கை அலுவலர் மூலம் கணினி தணிக்கை செய்ய வேண்டியது மிகவும் அவசியமாகும்.

TBA முறையில் உள்ள குறைபாடு

இந்த முறையில் ஒவ்வொரு கிளையில் உள்ள கணக்கு விவரங்கள் அந்தக் கிளையில் உள்ள சர்வரிலேயே பாதுகாக்கப்படுகின்றன. எனவே ஒரு கிளை வாடிக்கையாளர் அதே வங்கியின் மற்றொரு கிளையில் இருந்து அவரது கணக்கில் பரிவர்த்தனை செய்ய இயலாது.

மேலும் தரவு பாதுகாப்பிற்காக தினமும் அனைத்து கணக்கு விவரங்களும் குறுந்தகடு மற்றும் டேட்புகளில் சேமிக்கப்பட்டு (BACKUP) தலைமை அலுவலகத்திற்கு அனுப்பப்படவேண்டும்.

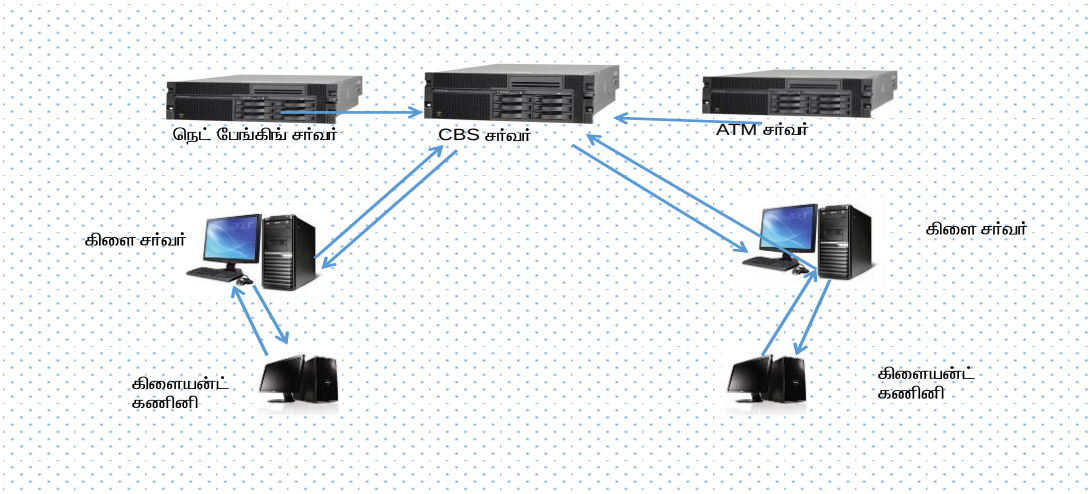
இதற்கு தீர்வாக மைய வங்கியியல் தீர்வு (CBS) என்ற தொழில் நுட்பம் அறிமுகப்படுத்தப் பட்டது.

(Core Banking Solutions - CBS)

மைய வங்கியியல் தீர்வு முறையில் ஒரு வங்கியின் அனைத்து கிளைகளும் நெட் வொர்க் மூலம் இணைக்கப்பட்டிருக்கும். அந்த வங்கியின் அனைத்து கிளைகளிலும் உள்ள அனைத்து கணக்குகளின் விவரங்களும் நாட்டின் ஏதாவது ஒரு இடத்தில் உள்ள தரவு தளத்தில்; (Data Base) வைக்கப்பட்டிருக்கும்.இதன் காரணமாக வாடிக்கையாளர் அவ்வங்கியின் வேறு எந்த ஒரு கிளையிலிருந்தும் அவரது கணக்கில் பற்று, வரவு செய்ய இயலும். எனவே வங்கிக் கிளையின் வாடிக்கையாளர் அவ்வங்கியின் வாடிக்கையாளர் ஆகிவிடுகிறார்.

மைய வங்கியியல் கட்டமைப்பு

மைய வங்கியியலில் பரிவர்த்தனை நடைபெறும் விதம்



மின்னணு பணப் பரிமாற்றம்

(ELECTRONIC FUND TRANSFER (EFT)

மைய வங்கியியல் தீர்வு முறையில் ஒரு வங்கியின் வெவ்வேறு கிளைகளில் உள்ள கணக்கு எண்களுக்கு இடையில் பணப் பரிமாற்றம் செய்யலாம். ஆனால் இம்முறையில் ஒரு வங்கிக் கணக்கிலிருந்து மற்றொரு வங்கிக் கணக்கிற்கு நேரடியாக பணப் பரிமாற்றம் செய்ய இயலாது.

இதற்கு தீர்வாக மின்னணுப் பணப் பரிமாற்ற முறையில் ஒரு வங்கிக் கணக்கிலிருந்து மற்றொரு வங்கிக் கணக்கிற்கு இந்திய ரிசர்வ் வங்கியின் மூலம் பணப் பரிமாற்றம் செய்ய இயலும்.

இதில் இரண்டு வழி முறைகள் உள்ளன.

1) **NEFT (National Electronic Fund Transfer)**

2) **RTGS (Real Time Gross Settlement)**

இம்முறையில் பணப் பரிமாற்றம் (IFSC)என்ற குறியீடு பயன்படுத்தப்படுகிறது.இதன் மூலம் ஒரு வங்கி மற்றும் அதன் கிளையை அறிந்து கொள்ள இயலும்.

இது ஒரு பதினோரு இலக்க எண்ணாகும்.இதன் முதல் நான்கு இலக்கங்கள் ஆங்கில எழுத்துகளைக் கொண்டு அந்த வங்கியை அறிவதற்கு பயன்படுகிறது. ஐந்தாவது இலக்கம் "0" மாக (பூஜ்ஜியமாக) இருக்கும். கடைசி 6 இலக்கங்கள், எண்களைக் கொண்டு, அந்த வங்கியின் கிளையை அறிய பயன்படுகிறது.

NEFT:

- இந்த முறையில் ஒரு நாளில் காலை 8.00 மணியிலிருந்து மாலை 7.00 மனி வரையில் தொகுப்பு முறையில் ஒவ்வொரு அரை மணி நேரமாக, 23 முறை பணப் பரிமாற்றம் நடைபெறுகிறது.

- ஒரு கணக்கு எண்ணிலிருந்து மற்றொரு கணக்கு எண்ணிற்கு பணப் பரிவர்த்தனை செய்வதற்கு எந்தவித பண அளவு வரம்பும் கிடையாது.

- பணத்தைப் பெற்றுக்கொள்ளும் வங்கியானது இரண்டு மணி நேரத்திற்குள் வாடிக்கையாளரின் கணக்கில் வரவு வைக்க வேண்டும்.

RTGS:

- இந்த முறையில் ரூபாய் இரண்டு இலட்சம் மற்றும் அதற்கு மேலான பணப் பரிவர்த்தனை செய்யப் பயன்படுகிறது.
- காலை 8.00 மணி வரை ஒரு வங்கிக் கணக்கிலிருந்து மற்றொரு வங்கிக் கணக்கிற்கு பணப் பரிமாற்றம் உடனுக்குடன் செய்யலாம்
- பணத்தைப் பெற்றுக் கொண்ட வங்கியானது 30 நிமிடத்திற்குள் வாடிக்கையாளர் கணக்கில் வரவு வைக்க வேண்டும்.
- குறிப்பிட்ட கால அளவிற்குள் வாடிக்கையாளர் கணக்கில் வரவு செய்யாவிடில், பணத்தைப் பெற்றுக்கொண்ட வங்கியானது தண்டத்தொகை (Penalty)செலுத்த நேரிடும்.

NEFT, RTGSமுறையில் பணப் பரிவர்த்தனை செய்வதற்கு பணம் செலுத்த வாடிக்கையாளர் கீழ்க்கண்ட தகவல்களை அதற்கான விண்ணப்பத்தில் பூர்த்தி செய்ய வேண்டும்.

1) அனுப்ப வேண்டிய தொகை
2) பற்று செய்ய வேண்டிய பணம் அனுப்புபவரின் கணக்கு எண்
3) பயனாளி வாடிக்கையாளரின் வங்கி மற்றும் அதன் கிளையின் பெயர்
4) பணம் சென்று சேர வேண்டிய வங்கியின் IFSC குறியீடு
5) பயனாளி வாடிக்கையாளரின் பெயர்
6) பயனாளி வாடிக்கையாளரின் கணக்கு எண்
7) அனுப்புபவரிடமிருந்து பெறுபவருக்கு அனுப்ப வேண்டிய தகவல் ஏதாவது இருப்பின்

NEFT மற்றும் RTGS முறையில் வங்கியின் வேலை நாள் மற்றும் வேலை நேரத்தில் மட்டுமே பணப் பரிவர்த்தனை செய்ய முடியும்.

உடனடி பணப் பரிவர்த்தனை சேவை

(Immediate Payment Service - IMPS)

IMPSசேவையை ரிசர்வ் பேங்க் ஆப் இந்தியா (RBI) மற்றும் இந்தியன் பேங்கர்ஸ் அசோசியேசன் (IBA) ஆகியவை இணைந்து ஏற்படுத்தி இருக்கும் நேஷனல் பேமண்ட்ஸ் கார்ப்பரேஷன் ஆப் இந்தியா (NPCI) வழங்குகிறது.

IMPSசேவை மூலம் ஒரு வங்கிக் கணக்கிலிருந்து மற்றொரு வங்கிக் கணக்கிற்கு உடனுக்குடன் ஒரு நாளின் 24 மணி நேரமும் பணம் அனுப்ப முடியும். (24 X 7 X 365)

IMPSமூலம் கீழ்க்கண்ட சேவைகளைப் பெற முடியும்.

1) பணம் அனுப்புதல்
2) பணம் பெறுதல்
3) வணிக நிறுவனங்களுக்கு பணம் செலுத்துதல்
4) பயணச் சீட்டிற்கு பணம் செலுத்துதல்
5) கடன் அட்டைக்கு பணம் செலுத்துதல்
6) கல்லூரி மற்றும் பள்ளிக் கட்டணம் செலுத்துதல்
7) இணையதள வர்த்தகம் செய்தல்

IMPS மூலம் பணப் பரிமாற்றத்தை கீழ்க்கண்ட சேனல்கள் மூலம் செய்யலாம்.

i) கைபேசி (Mobile Phone)
ii) வலையதளவங்கிச் சேவை (Internet Banking)
iii) ATM

கீழ்க்கண்ட முறைகளில் IMPSபரிவர்த்தனை செய்ய இயலும்.

1) பயன் பெறுபவரின் கைபேசி எண் மற்றும் எம்.எம்.ஐ (MMID)
(MMIDஎன்பது மொபைல் மணி ஐடெண்டிபையர் என்பது ஒரு 7 இலக்க எண். இந்த எண் பயனாளியின் கைபேசி எண். எந்த வங்கியில் உள்ள கணக்கில் இணைக்கப்பட்டுள்ளதோ அந்த வங்கியால் வழங்கப்படுகிறது. ஒரு கைபேசி எண்ணிற்கு வெவ்வேறு வங்கியின் MMID–க்களை பெற முடியும்)

2) பயன் பெறுபவரின் கணக்கு எண் மற்றும் ஐ.எப்.எஸ். குறியீடு (IFSC)
3) பயன் பெறுபவரின் ஆதார் எண்

பணப் பரிவர்த்தனை வரம்பு–

IMPSமூலம் ஒரு நாளைக்கு ரூபாய் இரண்டு இலட்சம் வரை பணப் பரிமாற்றம் செய்ய இயலும்.

*99 #சேவை

*99 #சேவை எ;னபது NPCI–ஆல் தொடங்கப்பட்ட ஒரு எளிமையான பணப் பரிவர்த்தனை சேவை ஆகும்.

இந்தச் சேவை USSD (அன்ஸ்ரக்சர்டு சப்ளிமெண்டரி சர்வீஸ் டேட்டா) தொழில் நுட்பத்தில் வேலை செய்கிறது. இந்த தொழில் நுட்பம் GSM (குளோபல் சிஸ்டம் பார் மொபைல் கம்யூனிகேஷன்ஸ்) கைபேசிக்காக பிரத்யேகமாக உருவாக்கப்பட்டது.

***99 #சேவையின் அம்சங்கள் :–**

1) இணையதள வசதி இல்லாமல் செயல்படிக்கூடியது.
2) தொலைபேசி சேவை வழங்கும் எல்லா நிறுவனத்திடமும் ஒரே குறியீடாக *99 #ஐ பயன்படுத்தலாம்.
3) இந்த சேவைக்கு குறுந்தகவலுக்கான (SMS) கட்டணம் மட்டுமே வசூலிக்கப்படும்.
4) இந்த சேவையை பயன்படுத்தும் பொழுது ரோமிங் கட்டணம் கிடையாது.
5) 24 மணி நேரமும் சேவையை பெற முடியும்.
6) இந்த சேவையை பெறுவதற்கு கைபேசியில் எந்த ஒரு செயலியையும் பதிவிறக்கம் செய்யத் தேவையில்லை.

இச்சேவையின் மூலம் அரசின் நோக்கமான அனைவருக்கும் நிதிச் சேவை என்ற இலக்கை அடைய முடியும்

*99 #சேவை மூலம் கீழ்க்கண்ட சேவைகளை பெற முடியும்.

1) நிதி சார்ந்த சேவைகள்
2) நிதி சாரா சேவைகள்
3) மதிப்பு கூட்டப்பட்ட சேவைகள்

1) நிதி சார்ந்த சேவைகள்:–

a) **P2P (Person to Person)**ஒரு நபரிடமிருந்து மற்றொரு நபருக்கு பயனாளியின் கைபேசி எண் மற்றும் **MMID**மூலம் அனுப்ப முடியும்.

b) **P2A (Person to Account)**பயனாளியின் கணக்கு எண் மற்றும் IFSC மூலம் பணத்தை அனுப்பலாம்.

c) **P2U (Person to UIDAI)**பயனாளியின் ஆதார் எண் மூலம் ஆதார் எண் இணைக்கப்பட்டுள்ள வங்கிக் கணக்கிற்கு பணத்தை அனுப்ப இயலும்.

2) நிதி சாரா சேவைகள்:–

- கணக்கு எண்ணில் உள்ள நிலுவைத் தொகை அறிதல்.
- கணக்கின் குறு அறிக்கையை பெறுதல்; (Mini Statement)
- உபயோகிப்பாளரின; **MMID**அறிதல்
- MPIN (Mobile Personal Identification Number)உருவாக்குதல்;.
- MPIN-ஐ மாற்றுதல;
- ஒரு முறை மட்டும் உபயோகிக்கக் கூடிய கடவுச் சொல் (OTP) உருவாக்குதல;

3) மதிப்புக் கூட்டப்பட்ட சேவைகள;:-

QSAM (Query Service on Aadhar Mapper)சேவை.

***99 *99** #சேவை.இச்சேவை மூலம் உபயோகிப்பவரின் ஆத்ார் எண் எந்த வங்கியின் கணக்கு எண்ணுடன் இணைக்கப்பட்டுள்ளது என்பதை அறிய முடியும்.

<u>பணப் பரிவர்த்தனை வரம்பு</u>:-

***99** #சேவையின் மூலம் ஒரு பரிவர்த்தனையில் ரூபாய் ஒன்று முதல் ரூபாய் 5000/– வரை பணத்தை மாற்ற இயலும்.

ஒருங்கிணைக்கப்பட்ட பணப் பரிமாற்ற இடைமுகம்

(Unified Payment Interface - UPI)

இது ஒரு கைபேசி செயலி ஆகும்.

- 24 மணி நேரமும் உடனுக்குடன் பணப் பரிமாற்றம் செய்ய இயலும்.
- உபயோகிப்பாளர் அவருடைய மெய்நிகர் முகவரியை (Virtual Payment Address)ஏற்படுத்திக் கொள்ள முடியும்.
- மெய்நிகர் முகவரி என்பது உபயோகிப்பாளரின் கணக்கு எண்ணைக் குறிக்கக் கூடிய **email**–IDபோன்ற ஒரு தனிப்பட் முகவரி ஆகும். உதாரணமாக ஸ்டேட் பேங்க் ஆப் இந்தியாவில் உள்ள கணக்கு எண்ணிற்கு உருவாக்கப்படும் மெய் நிகர் முகவரி பெயர் @sbiஅதாவது ramesh@sbi என்று இருக்கும்.
- UPIமூலம் பணப் பரிமாற்றம் செய்யும் பொழுது பயனாளியின் கணக்கு எண்ணை முதலிலேயே பதிவு செய்திருக்கத் தேவையில்லை.
- UPIமூலம் கீழ்க்கண்ட வழிகளில் பணப் பரிமாற்றம் செய்யலாம்.

1) பயனாளியின் மெய்நிகர் முகவரி மூலம்
2) பயனாளியின் கணக்கு எண் மற்றும் IFS Code மூலம்
3) பயனாளியின் கைபேசி எண் மற்றும் MMIDமூலம்
4) பயனாளியின் ஆதார் எண் மூலம்

UPI – PIN

UPI - PINஎன்பது ஒரு 6 இலக்க கடவுச் சொல். இது நாம் முதல் முறையாக UPIசெயலியில் பதிவு செய்யும் பொழுது நம்மால் உருவாக்கப்படுவது UPIமூலம் பணப் பரிவர்த்தனை செய்யும் பொழுது இந்த எண்ணை உபயோகப்படுத்த வேண்டி இருக்கும்.

பணப் பரிவர்த்தனை வரம்பு:-

UPIமூலம் ஒரு நாளைக்கு ரூபாய் ஒரு இலட்சம் வரை பணப் பரிமாற்றம் செய்ய இயலும்.

பீம் செயலி (BHIM-APP)

பாரத் இண்டர்பேஸ் பார் மணி என்பது ஒரு கைபேசி செயலி ஆகும். இதன் மூலம் ஒரு வங்கிக் கணக்கிலிருந்து மற்றொரு வங்கிக் கணக்கிற்கு உடனுக்கடன் 24 மணி நேரமும் பணப் பரிமாற்றம் செய்ய முடியும்.

இந்தச் செயலியின் மூலம் கீழ்க்கண்ட சேவைகளைப் பெற முடியும்.

1) பணம் அனுப்புதல்;:-

உபயோகிப்பாளர் கீழ்க்கண்ட வழிகளில் பணத்தை அனுப்ப முடியும்.

a) மெய்நிகர் முகவரி (VPA)

b) கணக்கு எண் மற்றும் IFS Code

c) பயனாளியின் ஆதார் எண்

d) QR Code

2) பணம் கேட்டுப் பெறும் வசதி (Request Money)

உபயோகிப்பாளர் மெய் நிகர் முகவரி மூலம் பணம் பெறுவதற்கான கோரிக்கையை அனுப்பலாம்.

3) ஸ்கேன் செய்து பணம் அனுப்பும் முறை:-

உபயோகிப்பாளர் QR Code–ஐ ஸ்கேன் செய்து பணத்தை அனுப்ப முடியும்.

இந்த செயலியில் உபயோகிப்பாளர் தனது மெய் நிகர் முகவரியை மற்றொரு வங்கிக் கணக்குடன் இணைக்கலாம்.

பீம் செயலியை உபயோகிப்பதற்கான வழிமுறைகள்;:-

Step–1

பீம் செயலியை கூகுள் பிளே ஸ்டோர் மூலம் பதிவிறக்கம் செய்து கொள்ள வேண்டும்.

Step–2

உபயோகிப்பதற்கான மொழியை தேர்வு செய்ய வேண்டும் (தற்போது 13 மொழிகளில் ஏதாவது ஒன்றை தேர்வு செய்யலாம்).

Step–3

வங்கிக் கணக்கில் இணைக்கப்பட்டுள்ள கைபேசி எண்ணை கொண்டுள்ள சிம் கார்டை தேர்வு செய்ய வேண்டும்.

Step–4

செயலியில் உள் நுழைவதற்கான கடவுச் சொல்லை உருவாக்க வேண்டும்.

Step–5

கணக்குஎண் விருப்பப்பட்டியல் **(Option)** மூலம் தேவையான வங்கிக் கணக்கு எண்ணை இணைக்க வேண்டும்.

Step–6

வங்கியின் பற்று அட்டையின் கடைசி 6 எண்கள் மற்றும் அட்டையின் முடிவு காலம் **(Maturity Date)** ஆகியவற்றைக் கொண்டு **UPI Pin**–ஐ உருவாக்க வேண்டும்.

Step–7

நமது கைபேசி எண்**@UPI**என ஒரு மெய் நிகர் முகவரி(**e.g. 94441 09125 –UPI**) தாமாகவே உருவாகிவிடும்.

பணப் பரிவர்த்தனை வரம்பு–

பீம் செயலியின் மூலம் ஒரு பரிவர்த்தனையில் ரூபாய் 10,000/– வரையிலும், ஒரு நாளைக்கு சுமார் ரூபாய் 20,000/– வரையிலும் பணப் பரிமாற்றம் செய்ய இயலும்.

COMPUTER SECURITY

1. Objective
2. Physical Security
3. Logical Security
4. Network Security
5. Biometric Security

1.OBJECTIVE

The number of computer networks is growing rapidly and also the number of instructions. With increasing economic importance of computer networks, the extent of criminal activates is also growing. Banks have to take precautions to protect form the risks. The objective of this is to make the reader understand the different computer security environment and security mechanisms. To know the controls required to deploy at physical, logical and network levels.

2. **PHYSICAL SECURITY**

The point of controlling physical access to information systems to prevent unauthorized persons to cause system security incident is likely to exploit vulnerability. Giving someone an opportunity to cause system security incident is likely to result in some form of loss and is a poor management practice.

The aspects of physical security are intrusion prevention, intrusion detection, proper information destruction, document security, power protection, water protection, water protection, fire protection and contingency planning. ***Disturbance sensors :*** These are perimeter detection sensors, commonly are fence mounted.

Barrier detectors : These detection devices send forth a continuous beam of energy, a break in which indicates intruder penetration.

Buried - ***Line sensors :*** These are underground cables or instruments designed to sense pressure, seismic and magnetic signals.

Capacitance sensors : These are for small distance. The shift in the capacitance, in response to a physical presence in near vicinity, triggers corresponding changes in dielectric characteristics in the field between the capacitor plates.

Surveillance: This is accomplished through the use of radar or Closed Circuit TV (CCTV).

More often people talk about computer acquirement about PC Security and the problems with equipment theft, they immediately thick about the cost replacing lost or damaged equipment, But they often forget the data stored stolen computers. In fact, the software and data stored on personal

Computers and Lap - Tops is of much greater value than the equipment itself. Apart from the fact the data may be confidential or sensitive, one has to consider the cost of replacing the lost software and data form backup files or if the files were not backed up, rebuilding all files databases from scratch, that is the real cost of replacing stolen computers!

- Apart from the cost of replacing the equipment, an even bigger problem is getting the replacement equipment to a state where it can be used productively. One also needs to consider the loss of productivity and possibly business opportunity until the equipment is replaced and it's ready for use.
- Make sure that all software, date and databases are backed up regularly and that backup media is stored in a safe, protected and secure place.
- If the computer / lap - top is used to store confidential or sensitive information, consider encrypting the information so that the data cannot be accessed even if the equipment is stolen.
- Consider installing an intrusion detection alarm system protect the premises and contents.
- Encourage employees to challenge strangers entering officer areas. Employees should also be instructed to ask for identification from all services. Maintenance, and delivery personnel.
- Consider using anchoring pads, security cables or an equipment alarm system to prevent the equipment
- Make sure there is a complete and detailed inventory of all equipment and software.

Document Security

- Inventory all records to determine which are vital to the bank.
- Identify which departments and / or employees are responsible for all vital records.
- Establish retention, classification, storage and disposal standards for all vital records.
- Conduct periodic reassessments of all vital records to ensure that they are still valid.
- Consider transferring vital records to microfilm / fiche or CD - ROM.
- Store paper records in acid - free cardboard cartons or plastic containers.

- Implement the appropriate safeguard strategies for vital records stored on electronic / magnetic media.
- Store vital records at an off - site location away your officers. Make sure that off-site facilitates provide adequate security and protection for your records.

Power supply : Power is critical to computing environment. Although we often take power supply to computing equipment can result in loss or corruption of date and loss of availability. This is true though many fluctuations are not noticeable to the average user. In mainframe environment, it is common to provide protection of computing equipment through UPS (Uninterruptible Power Supply) systems, connection to two different power grids, and in some cases diesel generators.

1. LOGICAL SECURITY

Logical Security is related to software to software access controls. Software success controls generally act as barriers between users and protected resources. The process of access control is based on tow points of authorization and authentication. Authorization is carried out by a responsible official, Who determines and grants need - based rights to individual users. Authentication is the actual verification to the identity of the user who is attempting to login. Password technique is the popular mode of granting entry to the system. Use of time - tested encryption methods can also go hand in hand with the use of passwords.
Some computer systems may require additional security features for particular application, which are generally supported by the operating system. These can be classified as under.

(a) Multiple types of acces control - at user level, terminal level, menu level, field level and application level.

(b) Internal access controls - based on information such as date, time, terminal location, and user identification.

(c) Limiting the number of unsuccessful tries and locking out the requester and simultaneous broadcasting of such event to all users.

(d) Automated audit trail of tracking of access situations.

(e) Limiting privileged access on directories and utilities.

(f) Encryption of date and files.

The selection of software security is based on the existing computer application environment, the ease and accuracy of installation, capability to support operational environment, and maintenance.

Security Code Generators : A bunch of hardware access controls devices, variously referred to as security key generators, see - through security devices, hand - held keys, decoders, and access - control encryption card, which would monitor delivery of a 'One - time' password or coordinating host. Here, the advantage over conventional passwords is prevention of observation and reentry of an intercepted password. The Security code generator process employs a technique that causes successive password entered by a user to differ in unpredictable ways. The generation of security codes or passwords is aided by a hand - held device carried by the user.

Smart Cards : These are cards that contain a microprocessor or equivalent means of logically processing date, a memory for storing data and dedicated security logic. Some smart cards even have keypads, a screen and internal power in addition to the usual smart card features. The smart cards are self - verifying security cards used power in addition Viz., Debit cards, credit cards, telephone charge cards and record repositories.

Access Controls

Access Controls: are controls designed to prevent, or limit the likelihood, of unauthorized access to data files or programe. Access controls which can be built into a system's software are :

(a) Passwords

(b) Personal identification of the user, and

(c) Encryption and authentication.

Passwords

Passwords are 'a set of characters which may be allocated to a person, a terminal or a facility which are required to be keyed into the system before further access is permitted'. Passwords can be applied to date files as well as program files. The terminal users can be restricted to the use of certain files and programs (e.g.in banking system, clerical grade staff are allowed to access certain routine programs only.

The restriction of access to a system with password is effective and widely used but the widespread and growing use of personal - computers and distributed systems is making isolation virtually impossible. The wider use of information systems requires that access to the system becomes requirements for access a rigidly enforced isolation of the system may significantly reduce the value of the system.

Virtually all multiuser systems use passwords. In order to access a system the user needs first to enter a string of characters as a 'Password'. If the entered password matches one issued to an authorized user the system permits access.

Some system - software (e.g. Oracle) comes with default password. It is essential that theses be changed if the system is to be at all secure. This is particularly important to guard against external penetration of the security system since such common passwords may become widely known to the people.

Passwords ought to be effective in keeping out unauthorized users, but they are by no means foolproof. Experience has shown that unauthorized access can be obtained.

(a) By experimenting with possible passwords, an unauthorized can gain access to a program or file by guessing the correct password. This is not as difficult, it may seem when many computer users specify ' obvious' passwords.

(b) Someone who is authorized to access the system may tell an unauthorized person what the password is, perhaps through carelessness.

The main drawback to using password is that they rely upon to use them conscientiously. Passwords need to be random since the easily - remembered passwords are also highly predictable. Therefore a password system requires both a software and strong organizational policies if is to be effective.

All attempted violations of security should be automatically logged and the log checked regularly. In many new multiuser systems, the terminal from where the unauthorized user attempting the violation may be automatically disconnected, or that account will be automatically locked by the system after a certain number (say 3) of unsuccessful attempts.

PINs

In some systems, the user might have a special PIN (Personal Identification Number) which Identifies him or her to the system. According to what the user's PIN is, the user will be allowed access to certain part of the systems, but forbidden access to other parts. An example of authorization systems with PINs is cards for banks' each dispensers. The cash dispenser checks the PIN code on the magnetic strip of the card against the code number keyed in by the cardholder, and codes must match before the cardholder is allowed to withdraw any cash

Encryption and Authentication

When date is transmitted over a telecommunication link of network, there are two main security dangers, unauthorized access by an eavesdropper, and direct intervention by someone who sends false message down the line, claiming to be someone else - so that the recipient of the message will thick that it has come from an authorized source.

Encryption is the only secure way to prevent eavesdropping (since eavesdroppers can get passwords by tapping the line or by experimenting with various likely passwords). Encryption involves scrambling the data at one end of the lineal transmitting the scramble data, and unscrambling it at the receiver's end of the line

Authentication is a technique of making sure that a message has come from an authorized sender. Authentication involves addition an extra field to a record, with the contents of this field derived from the remainder of the record by applying an algorithm that has previously been agreed between the senders and the recipients of date.

4. NETWORK SECURITY

While network environment has definite advantage over the stand - alone systems, the security risk involved is also higher. The very Physical range of networks spawns a lot of problems, requiring greater protection against intruders / infiltrators. An instruction is somebody attempting to break into or misuse systems.

The primary ways an intruder can get into a system are :

(a) ***Physical Intrusion :*** if an intruder has physical access to a machine (i.e.they can use the keyboard or take apart the system), they will be able to get it. Techniques range from special privileges the console has, to the ability to Physically take apart the system and remove the disk drive (and read /write it on another machine)

(ii) System Intrusion : This type of hacking assumes the intruder already has a low - privilege user account on the system. If the system doesn't have the latest security patches, there is a good chance the intruder will be able to use a known exploit in order to again additional administrative privileges/

(Hi) Remote Instructions: This type of hacking an intruder who attempts to penetrate a system remotely across the network. The Intruder begins with no special privileges. There are several forms of this hacking. For example, an intruder has a much more difficult itme if there is a firewall between him / her and the victim machine.

The threats in a typical local are network include: Impersonation, eavesdropping, date alteration and Denial of Service.

Impersonation : If refers to the possibility of some one sending a message, which appears to have been sent from someone else. This can threaten contractual messages, such as orders and invoices. In a network environment, Om[resomation can take forms such a s- forging the ' sender' field in en e-mail message, falsifying the source IP address for establishing a network connection, or hijacking an existing connection between two computers.

Eavesdropping : It refers to the possibility of date being read by someone other than the intended recipients. For example, a competitor may intercept your proposal to a bid or your department plans. Generally, eavesdropping is simpler for an attacker to accomplish than impersonation, and is hardr to dtect.

Date Alteration : It refers to the risk of interception that results in tempering with date, that is, the possibility of date being changed in such a way it appears legitimate, but no longer represents the originators' intention, For example, the intruder may change a 'buy' order to 'sell', or adding to a bid.

Denial - ***of -service (DoS) attacks :*** where the intruder attempts to crash a service (or the machine), overload network links, overloaded the CUP, or fill up the disk. The intruder is not trying to gain information, but to simple act as a vandal to prevent from making use of machine.

An Intrusion Detection System (IDS) is a system for detecting such intrusions. IDS can be broken down into the following categories.

(a) Network intrusion detection systems (NIDS) monitors packets on the network wire and attempts to discover if a hacker / cracker is attempting break into a system or cause a denial of service attack.

(b) System integrity verifiers (SIV) monitors system files to find when and intruder changes them, thereby leaving behind a backdoor. One such famous system is 'Tripwire'. A SIV may watch other components as well, such as the windows registry and configurations, in order to find well-known signatures. It may also detect when a normal user somehow acquires root/administrator level privileges.

(c) Log file monitors (LFM) Monitor log files generated by network services. In a similar manner to NIDS, these systems look for pattern in the files that suggest an intruder in attacking. A typical example would be parser for HTTP server log files that looking for intruder who try well - known Security holes.

The intrusions may be detected by using the methods of

(a) Anomaly detection

(b) Signature recognition

(a) ***Anomaly detection*** : The most common way people approach network intrusion detection is to detect statistical anomalies. The idea behind this approach is to measure a " baseline" of such stats as CPU utilization, disk activity, user logins, file activity, and so forth. Then, the system can trigger when there is a deviation from this baseline. The benefit of this approach is that it can detect the anomalies without having to understand the underlying cause behind the anomalies. For example, let's say that you monitor the traffic from individually workstations. Then, the system notes that at let's say that you monitor the traffic from individual workstations. Then, the system notes that at 2am, a lot of these workstations start logging into the serves and carrying out tasks. This is something interesting to note and possibly take action on.

(b) ***Signature recognition :*** The majority of commercial products are based upon examining the traffic looking for well - known patterns of attack. This means that for every hacker technique, the engineers code something into the system for that techniques. This can be a simple as a pattern match.

The classic example is , every packet on the wire for the pattern " / cgi-bin/phf?", which might indicate somebody attempting to access this vulnerable CGI script on a web - server. Some IDS systems are built from large databases that contain hundreds or thousands of such strings. They just plug into the wire and trigger on every packet they see that contains one of these strings.
Other network security measures besides IDS are :

Firewalls : The firewall refers to network connecting an internal private corporate network to an external, public network such as internet, The aim of firewall system is to protect corporate network users form outside attack most people think of the firewall as their first line of dense. This means if intruders figure out how to bypass it (easy, especially since most intrusions are committed by employees inside the firewall), they will have free run of the network. A better approach is to thick of it as the last line of defence. Make sure machines are configured right and intrusion detection is operating, and then place the firewall up just to avoid the winnable script - kiddies. Note that routers these days can be configured with some firewall filtering. While firewalls protect

external access, they leave the neteowrk unprotected from internal intrusions. It has estimated that 80% of losses due to " hackers" have been internal attacks.

VPNs (Virtual Private Networks) : VPN crates a secure connection over the internet for remote access (e.g. for telecommutes). Example 1 :Microsoft includes a technology called PPTP (PPP Over TCP) built into Windows. This gives a machine two IP addresses. One on the Interenet, and a virtual one on the corporate network. Example 2 : IPsec enhances the traditional IP Protocol with security.
Encryption : Encryption is becoming increasingly popular in secure message transmission, in which the message is transformed into an ineligible character string and transmitted over the network. We have choice of e-mail encryption (PGP, SMIME), file encryption (PGP again), or file system encryption (BestCrypt, PGP again).

Lures/honey pots : Programs that pretend to be a service, but which do not advertise themselves. It can be something as simple one of the many Back office emulators, or as complex as an entire subnet of bogus systems installed for intruder detection purpose.

5. BIOMETERIC SECURITY

Biometric Characteristics of a person can be other than biological characteristics like fingerprints. These can include automated measurements of personal performance, where the performance characteristics are unique to a person. The automation generally consists of transuding some analog measurement of a physical or behavioral characteristic, converting converging the analog 'signal' (Voltage, current, Optical, Or infracted intensity) to a digital sequence, processing the sequence through some algorithm, usually proprietary and try to match the output to a catalog of reference records.

The following are the widely used biometric techniques :

Signature Recognition: Signature is the most commonly used mode of identity verification, But the ordinarily discernible pattern is not the one biometric signature recognition systems depend on Biometric signature devices operate by signature dynamics, i.e., how a signature is written and not as the pattern indicates. It takes into account the time, history of pressure, velocity, direction and acceleration. Several Signatures are needed for initial registration and recognition. Characteristics can be averaged, as it has been observed that individual portions of a signature may differ more than the parameter average. One device makes us of a ballpoint pen, directly evaluation pressure and velocity on the writing

surface. The salient requirements of signature verification are user ease, familiarity and adequate accuracy.

Fingerprint Recognition : of all biometric characteristics, fingerprints are supposed to be most unique, Fingerprints are images of papillary ridges in the outer skin layer of fingers. Reasonable accuracy and ease of measurement are the hallmarks of fingerprint verification. And these methods for identification purpose have been used from ancient times by law enforcement authorities, especially the British government, which classified, field and used fingerprints for systematic identification. Like in the case of a signature, it is better to register more than one finger, as a measure of precaution in the event of finger injury of a soiled finger.

Palmprint Recognition : Palmprints are similar to fingerprints, but a larger area of operation and more extensive features and hence are easier than fingerprints for verification purpose.

Hand - geometry Recognition : Hands are the next logical step in biometrical identification process and hands offer several measurable physical charterisiotcs that are unique to an individual. These devices operate by measuring a three dimensional image of the hand. In case of injury or fingernail length change, reenrollment might be an occasional requirement.

Voiceprint Recognition : This type of biometric device is based on the principal of voice recognition, akin to that on telephone. One of the techniques develops a time - dependent correlation and mannerism records. Security features include techniques to combat the use of tape recordings for spoofing.

Eye Retina Pattern Recognition : From the viewpoint of an ophthalmologist the retina patterns are quite unique. This fact has been advantageously utilized in biometric devices. The verification device uses an infrared beam to scan the back of the eye in a circular pattern and a detector measures the reflected light. If the measurement object maintains correct visual orientation, then the assement of the patter obtained is quite clear. This technique is also used in bank’s ATM access.

TNSC BANK

AGRICULTURAL CO-OPERATIVE STAFF TRAINING INSTITUTE

Sponsored by: THE TAMIL NADU STATE APEX CO-OP. BANK LTD

MADHAVARAM MILK COLONY, CHENNAI - 600 051.

TOPIC