AS DNB banka

DNB Link specifikācija
(B2B functional description)

DNB_LINK.FS.1.EXTSYS.1.L.2013

Saturs

1. DNB Link sistēmas mērķis

DNB Link sistēma nodrošina šādus biznesa procesus:

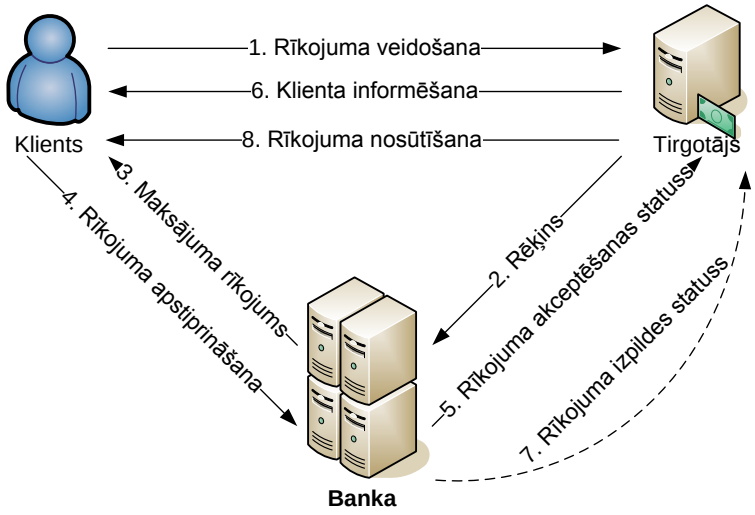
- Preču un pakalpojumu apmaksu (maksājumu veikšanu) – Pakalpojumu sniedzēji (turpmāk tekstā – Tirgotāji) var sūtīt savus Klientus uz internetbanku ar jau sagatavotiem maksājumu rīkojumiem un saņemt apstiprinājumu no bankas par veiksmīgu/neveiksmīgu rīkojuma (maksājuma) izpildi. Piemēram, veikt maksājumus par precēm interneta veikalos, apdrošināšanas kompānijās un citās sistēmās, izmantojot speciālo internetbankas interfeisu;
- Lietotāju autorizāciju ārējās sistēmās, izmantojot internetbanku;
- internetbankas lietotāja personas datu nosūtīšanu ārējām sistēmām.

2. Biznesa procesi

2.1. Preču un pakalpojumu apmaksa

Preču un pakalpojumu apmaksa ir iespējama tikai pie tiem Tirgotājiem, kas parakstījuši līgumu ar Banku par šāda pakalpojuma pieslēgšanu.

Preču un pakalpojumu apmaksas shēma ir parādīta Zīm. 1.



Zīm. 1 Apmaksas shēma

Process sastāv no sekojošiem posmiem:

1. Klients uzsāk procesu, kad izmanto interneta veikalu vai kādu citu ārējo sistēmu. Bankas klientam ir nepieciešama Web pārlūkprogramma, lai izvēlētos Tirgotāja preces / pakalpojumus un veiktu maksājumus, izmantojot internetbanku. Klients izvēlas noteiktas preces / pakalpojumus, kurus viņš vēlas iegādāties.
2. Tirgotājs piedāvā Klientam iespēju veikt maksājumu caur internetbanku, izveidojot HTML lapu, kura ģenerē maksājuma rīkojuma datus un pāradresē Klienta pārlūkprogrammu uz internetbankas serveri. Datu integritāte tiek nodrošināta ar Tirgotāja elektronisko parakstu.
3. Banka:
    a. Parāda internetbankas lapu, kurā Klientam tiek piedāvāts ievadīt lietotāja vārdu, paroli un kodu no kodu kalkulatora vai kodu kartes.
    b. Banka veiks Tirgotāja elektroniskā paraksta pārbaudi un tad Klients tiks aicināts apstiprināt gatavu un jau aizpildītu maksājuma rīkojumu.
4. Klients var apstiprināt jau sagatavoto maksājuma rīkojumu vai atgriezties Tirgotāja sākumlapā. Ja Klients atgriežas Tirgotāja sākumlapā, neapstiprinot maksājumu, maksājums netiks saglabāts internetbankas datu bāzē.
5. Pēc tam, kad Klients ir apstiprinājis rīkojumu, Banka:
    a. Nosūta Klientam informāciju par maksājuma rīkojuma statusu, kuras integritāte ir nodrošināta ar Bankas elektronisko parakstu, izsaucot lapu no Tirgotāja puses, izmantojot POST metodi.
    b. Ģenerē HTML lapu, kura satur informāciju par veiksmīgu maksājuma rīkojuma pieņemšanu apstrādē, un attēlo to Klientam.
6. Klients šajā lapā var:
    a. Atgriezties uz Tirgotāja lapu;

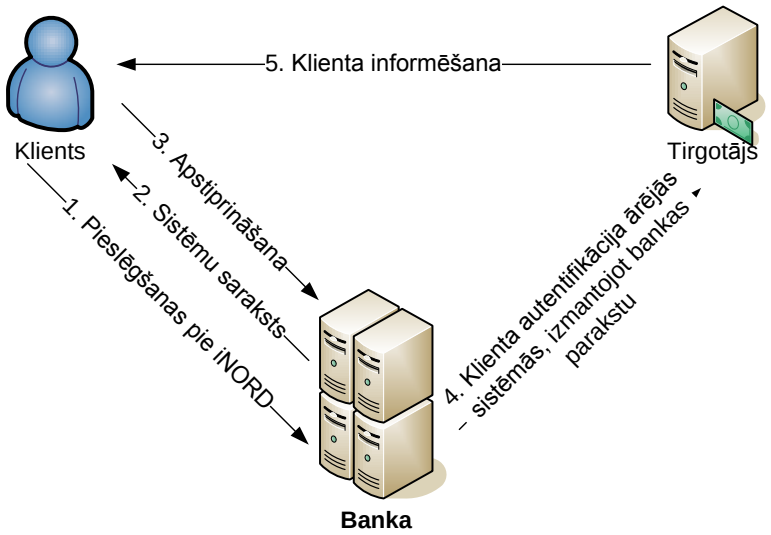
b. Turpināt darbu internetbankā;
c. Aizvērt Web pārlūkprogrammu.

Kļūdaina paraksta gadījumā sistēma atgriezīs atbilstošu kļūdas ziņojumu un neļaus nosūtīt maksājuma rīkojumu.

7. Pēc maksājuma rīkojuma izpildes vai atteikuma Banka pieprasa Tirgotāja noteikto lapu operācijas apstiprināšanai un nodot parametrus, izmantojot POST metodi. Operācija tiek izpildīta asinhroni.
8. Tirgotājs, saņemot no Bankas galīgo maksājuma statusu, pārbauda Bankas elektronisko parakstu un veic attiecīgus pasākumus. Piemēram, apstiprinājuma gadījumā, nosūta preces un pakalpojumus Klientam. Vai atteikuma gadījumā – dzēš rīkojumu.

2.2. Autorizācija ārējās sistēmās

Autorizācija ir iespējama tikai tajās ārējās sistēmās, ar kuru Bankai ir noslēgts līgums.
Autorizācijas shēma ir parādīta Zīm. 2.



Zīm. 2 Shēma: Autorizācija ārējās sistēmās

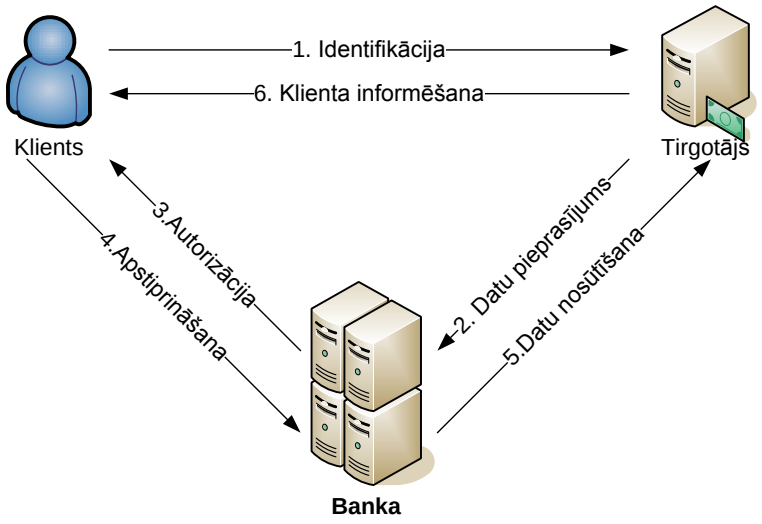
Process sastāv no sekojošiem posmiem:

1. Klients uzsāk procesu, autorizējoties internetbankā.
2. Banka piedāvā Klientam ārējo sistēmu sarakstu, kuras Klients var izvēlēties, noklikšķinot uz hipersaites.
3. Klients var apstiprināt datu pārraides faktu vai atcelt to. Klienta novirzīšana uz ārējo sistēmu ir iespējama tikai tad, kad Klients apstiprina personas datu pārsūtīšanas faktu.
4. Pēc apstiprināšanas Banka veic Klienta novirzīšanu uz pieprasīto sistēmu, atverot jaunu pārlūkprogrammas logu un apstiprinot pieprasījumu ar Bankas elektronisko parakstu.
5. Ārējā sistēma pēc Bankas elektroniskā paraksta pārbaudes autentificē Klientu un piedāvā Klientam attiecīgus pakalpojumus.

2.3. Klienta personas datu pārsūtīšana Tirgotājam

Klienta personas datu pārsūtīšana Tirgotājam ir iespējama tikai ar Klienta piekrišanu un tikai tiem Tirgotājiem, ar kuriem Banka ir noslēgusi līgumu par šāda pakalpojuma sniegšanu.

Shēma „Klienta personas datu pārsūtīšana Tirgotājam" ir parādīta Zīm. 3.



Zīm. 3 Shēma: Klienta personas datu pārsūtīšana Tirgotājiem

Process sastāv no sekojošiem posmiem:

1. Klients uzsāk procesu, izmantojot Tirgotāju interneta veikalus vai citas ārējās sistēmas.
2. Tirgotājs, ja ir nepieciešama Klienta identificēšana, piedāvā viņam apstiprināt viņa personas datus, izmantojot internetbanku. Tirgotājs izveido HTML lapu, kura novirza Klienta pārlūkprogrammu uz internetbankas serveri. Datu integritāti nodrošina Tirgotāja elektroniskais paraksts.
3. Banka:
    a. Parāda internetbankas lapu, kurā Klientam tiek piedāvāts ievadīt lietotāja vārdu, paroli un kodu no kodu kalkulatora vai kodu kartes, proti, autorizēties.
    b. Pārbauda Tirgotāja elektronisko parakstu un lūdz Klientu apstiprināt personas datu pārsūtīšanu Tirgotājam.
4. Klients var apstiprināt vai noraidīt datu pārsūtīšanu.
5. Gadījumā, ja Klients apstiprina datu pārsūtīšanu, Banka:
    a. Pārsūta Klienta personas datus Tirgotājam, šo datu integritāti nodrošina Bankas elektroniskais paraksts.
    b. Novirza Klientu uz Tirgotāja Web lapu.
6. Tirgotājs, pēc datu saņemšanas no Bankas, pārbauda Bankas elektronisko parakstu un veic attiecīgās darbības savā sistēmā.

3. Drošība

3.1. Vispārīgie principi

Lai nodrošinātu datu pārsūtīšanas drošību, sistēmai ir jāatbilst šādām prasībām:

- Savienojums starp Tirgotāju un Klientu tiek organizēts saskaņā ar drošības prasībām, kuras izvirza Tirgotājs;
- Tirgotājs sazinās ar Banku, izmantojot standarta HTTPS/SSL protokolu;
- Banka pieslēdzas Tirgotājam saskaņā ar drošības prasībām, ko izvirza Tirgotājs, proti, izmantojot HTTPS/HTTP protokolus;
- Klients sazinās ar Banku, izmantojot standarta HTTPS/SSL protokolu;
- Datos, kurus Banka nosūta Tirgotājam vai otrādi, jābūt elektroniskajam parakstam, kas tādējādi ļauj otrai pusei būt drošai par datu integritāti. Algoritms, kas ģenerē elektronisko parakstu, ir aprakstīts sadaļā 3.3. Dati papildus netiek kodēti.

3.2. Elektroniskais paraksts

Elektroniskais paraksts – tas ir svešas šifrētas informācijas fragmenta iestarpinājums datos. Pati pārsūtāmā informācija nav aizsargāta, proti, paliek atvērta un pieejama apskatīšanai tām personām, caur kurām tiek sūtīta.

Svešā šifrētā informācija tiek veidota, izmantojot divas metodes: *hash* funkciju (*hash function*), lai aprēķinātu kontrolsummu, un rezultātu parakstīšanu ar privāto atslēgu.

3.2.1. Kontrolsumma

Kontrolsumma ir līdzeklis, lai uzraudzītu pārsūtāmo datu integritāti. Princips ir tāds, ka izvadot informāciju tiek aprēķināta vērtība pēc noteikta algoritma. Šī vērtība (kontrolsumma) tiek nosūtīta kopā ar datiem. Pie datu ievades kontrolsumma tiek aprēķināta pēc tā paša algoritma un salīdzināta ar kontrolsummu pie datu izvades.

Lai izveidotu kontrolsummu tiek izmantots *hash* algoritms SHA-1. *Hash* funkcija darbojas tādā veidā, ka praktiski ir neiespējami izveidot divus dažādus parakstus ar vienu un to pašu kontrolsummu.

3.2.2. Parakstīšana

Parakstīšanu un paraksta pārbaudi veic, izmantojot divas atslēgas – privāto (slēgto) un publisko (atvērto). Publiskā atslēga ir visiem jūsu korespondentiem, bet privātā – tikai jums. Algoritms darbojas tādā veidā, ka parakstīšanai izmanto Tirgotāja privāto atslēgu un paraksta pārbaudei izmanto Tirgotāja publisko atslēgu.

Kontrolsumma, kas izveidota ar *hash* funkcijas palīdzību, ir šifrēta, izmantojot sūtītāja privāto atslēgu ar RSA algoritmu un nosūtīta kā pieprasījuma daļa. Kontrolsummas ģenerācijas algoritms ir aprakstīts sadaļā 3.3.

3.3. Elektroniskā paraksta ģenerācijas algoritms

Visi pieprasījumi – no Tirgotāja uz Banku, un otrādi – satur elektronisko parakstu. Elektroniskais paraksts tiek aprēķināts pēc sekojoša algoritma un ir atkarīgs no vaicājuma parametru un algoritma parametru vērtības. Izmantojamais algoritms ir noteikts līgumā starp Banku un Tirgotāju. Pieprasījuma parametri, kas būs jāiekļauj aprēķinā, ir atkarīgi no pieprasījuma tipa. Aprēķinātais elektroniskais paraksts tiks pārveidots simbolu virknē, izmantojot BASE64 kodu, un nosūtīts otrai pusei VK_MAC pieprasījuma parametrā.

Elektroniskā paraksta aprēķināšanu veic, izmantojot publiskās atslēgas RSASSA-PSS algoritmu ar SHA-1 *hash* algoritmu. Aprēķinā tiek ņemts vērā pieprasījuma parametru garums un tā saucamie pieprasījuma tukšie lauki.

SIGN(x1,x2,…,xn) := RSA(SHA-1(p(x1)|| x1|| p(x2)|| x2 || … ||p(xn)||xn),e,n)

kur:

- **||** – simbolu rindu konkatenācija;
- **x1, x2, …, xn** – pieprasījuma parametri;
- **p(xi)** – parametra garuma funkcija. Atgriež parametra garumu kā 3-ciparu skaitli papildinātu ar ‘0’ (nulle) no kreisās puses. Gadījumā, ja garums ir nulle, tiek atgriezts ‘000’;
- **e, n** – privātā atslēga, RSA parametri;
- Visiem pieprasījuma parametriem jābūt kodētiem ar UTF-8 kodējumu.

Piemērs:

Ir saņemts pieprasījums ar šādiem parametriem:

- VK_SERVICE=”1002”
- VK_VERSION=”101”
- VK_SND_ID=”MERCHANT”
- VK_STAMP=”1234567890”
- VK_AMOUNT=”6.79”
- VK_CURR=”EUR”
- VK_REF=”01012001-001”
- VK_MSG= ”Samaksa par precēm XXXXXX”

Elektroniskā paraksta aprēķināšana tiek veikta pēc simbolu virknes, ko veido šādi elementi (garums un vērtība šādiem parametriem):

- “0041002"
- ”003101”
- ”008MERCHANT”
- ”0101234567890”
- “0046.79”
- ”003EUR”
- ”01201012001-001”
- ”025Samaksa par precēm XXXXXX”

Vai kā vienu rindu:

“0041002003101008MERCHANT01012345678900046.79003EUR01201012001-

001025Samaksa par precēm XXXXXX”

Piemēram, ja VK_MSG parametrs būtu tukšs, tad parametru rindai būtu jābūt šādai: “00410020031010O8TIRGOTĀJS01012345678900046.79003EUR01201012001-001000”

3.4. Apmaiņas kārtība ar X509 sertifikātiem

Lai apmainītos ar X509 sertifikātiem:

1. Tirgotājs:
    a. Ģenerē abas atslēgas – privāto un publisko ar garumu 2048 bit, kā arī X509 sertifikātu;
    b. Saglabā privāto atslēgu savā sistēmā, lai parakstītu pieprasījumus Bankai;
    c. Laikā, kad paraksta līgumu ar Banku, iesniedz Bankai savu X509 sertifikātu;
    d. Saglabā saņemto no Bankas X509 sertifikātu savā sistēmā Bankas elektroniskā paraksta pārbaudei.
2. Banka:
    a. Ģenerē unikālas 2048 bit atslēgas - privāto un publisko, kā arī X509 sertifikātu Tirgotājam pirms līguma noslēgšanas;
    b. Saglabā savu privāto atslēgu savā sistēmā, piesaistot noteiktam Tirgotājam;
    c. Laikā, kad paraksta līgumu ar Tirgotāju, izsniedz viņam priekš viņa uzģenerēto X509 sertifikātu;
    d. Saglabā saņemto no Tirgotāja X509 sertifikātu savā sistēmā Tirgotāja elektroniskā paraksta pārbaudei.

X509 sertifikāti starp Banku un Tirgotāju tiek pārsūtīti PEM (Privacy Enhanced Mail) formātā. PEM formāts ir DER sertifikāts šifrēts BASE64, ievietotais starp rindām: "-----BEGIN CERTIFICATE-----" un "-----END CERTIFICATE-----".

Ierobežojumus attiecībā uz sertifikāta derīguma termiņu nosaka Banka. Sertifikāta derīguma termiņam ir jābūt – 3 gadi. Pirms sertifikāta termiņa iztecēšanas Banka un Tirgotājs vienojas par jaunu sertifikātu izveidošanu un apmaiņu.

4. Datu apmaiņas protokols

Datu apmaiņas protokols apraksta izsaukumu tipu un secību katram biznesa procesam. Izsaukumi ir HTTP POST pieprasījumi ar noteiktiem parametriem (laukiem).

Katrs pieprasījums satur pieprasījuma tipu. Katra pieprasījuma tipam atbilst obligāto parametru saraksts un apstrādes algoritms.

- Visi parametri, kas ir iekļauti pieprasījumā, ir obligāti. Obligātiem parametriem vienmēr jābūt iekļautiem pieprasījumā, pat ja to vērtības nav noteiktas (tukšs lauks);
- Summas pieprasījumos ir jānorāda, izmantojot punktu („.”) kā decimālo sadalītāju. Sadalītāju tūkstošiem neizmanto vispār;
- Datums jānorāda formātā „DD.MM.YYYY”, piemēram: „17.01.2010”;
- Laiks jānorāda formātā „hh24:mm:ss”, piemēram: „17:02:59”;
- Parametra vērtības garums nedrīkst pārsniegt maksimāli pieļaujamo, kas ir noteikts specifikācijā;
- Parametra vērtības garums var būt mazāks par maksimālo, nav nepieciešams, lai tiktu aizpildītas tukšas atstarpes. Parametra vērtība sākumā un beigās nedrīkst būt aizpildīta ar atstarpi („ ”);
- Nepareizi noformēti vai sabojāti pieprasījumi netiks apstrādāti;
- Darbībām, kuras tiek veiktas uz pieprasījuma pamata, jāatbilst pakalpojumu vispārējām prasībām (prasībām maksājuma rīkojumiem u.c.);
- Visiem datiem jābūt kodētiem UTF-8 kodējumā.

4.1. Pieprasījumi „Apmaksa par precēm un pakalpojumiem”

4.1.1. 1002. pieprasījums „Maksājuma rīkojuma dati”

Tirgotājs nosūta pieprasījumu Bankai. Pieprasījums satur datus par maksājuma rīkojumu, kurus Klients nevar izmainīt internetbankā. Šis pieprasījums ir nosūtīts ar POST metodi, izmantojot Bankas adresi, kad ir norādīta līgumā.

Tabula 1. 1002.pieprasījums „Maksājuma rīkojuma dati”

Nr.	Parametrs	Piedalās elektr. parakstā	Maks. garums	Apraksts	Skaidrojums
1.	VK_SERVICE	Jā	4	Pieprasījuma tips (1002)	1002
2.	VK_VERSION	Jā	3	Elektroniskā paraksta algoritms (101)	101
3.	VK_SND_ID	Jā	20	Tirgotāja ID	Tirgotāja identifikators bankā
4.	VK_STAMP	Jā	32	Pieprasījuma ID – unikāls numurs – (banka neizmanto)	Veido tirgotājs
5.	VK_AMOUNT	Jā	13	Maksājuma summa	Veido tirgotājs. Sadalītājs punkts (21.36)
6.	VK_CURR	Jā	3	Maksājuma valūta (EUR)	EUR
7.	VK_ACC	Jā	21	Saņēmēja konts	Tirgotāja konta numurs
8.	VK_NAME	Jā	105	Saņēmēja nosaukums	Tirgotāja vārds / nosaukums
9.	VK_REG_ID	Jā	20	Saņēmēja reģistrācijas numurs	Tirgotāja reģistrācijas numurs
10.	VK_SWIFT	Jā	20	Saņēmēja bankas kods	Tirgotāja bankas kods
11.	VK_REF	Jā	20	Maksājuma numurs Tirgotāja pusē	Veido tirgotājs
12.	VK_MSG	Jā	140	Maksājuma detaļas	Veido tirgotājs
13.	VK_RETURN	Jā	400	URL, kur novirzīt Klientu pēc maksājuma apstrādes	Veido tirgotājs
14.	VK_RETURN2	Jā	400	URL, kur sūtīt statusu pēc procesa beigām	Veido tirgotājs
15.	VK_MAC	Nē	300	Elektroniskais paraksts	Veido tirgotājs
16.	VK_TIME_LIMIT	Nē	19	Pieprasījuma termiņa beigu datums un laiks	Pēc šī datuma pieprasījums tiks uzskatīts par spēkā neesošu Formāts: 17.01.2010 12:00:00
17.	VK_LANG	Nē	3	Vēlamā valoda (LAT/ENG/RUS)	LAT

4.1.2. 1102.pieprasījums „Maksājuma statuss”

Tirgotājs saņem šādu pieprasījumu trīs reizes: pirmo reizi – tieši no Bankas servera pēc tam, kad maksājuma rīkojumu apstiprina Klients (parametri tiek nosūtīti, izmantojot POST metodi, izsaucot lapu Tirgotāja pusē, izmantojot adresi, kas norādīta 1002.pieprasījuma VK_RETURN2 parametrā, nosūtot statusu „1”); otro reizi – kad Klients pēc maksājuma apstiprināšanas atgriežas Tirgotāja mājas lapā (parametri tiek nosūtīti, izmantojot POST metodi, uz adresi, kas norādīta 1002.pieprasījuma VK_RETURN parametrā, nosūtot statusu „1”). Un trešo reizi – kad Bankas sistēma pabeidz maksājuma apstrādi (trešais izsaukums notiek, izsaucot lapu Tirgotāja pusē, izmantojot POST metodi parametru nosūtīšanai uz adresi, kas norādīta VK_RETURN2 parametrā. Statuss „2” vai „3” tiek nosūtīti atkarībā no tā, veiksmīgi vai neveiksmīgi tika apstrādāts maksājums).

Tirgotājs var saņemt šo pieprasījumu arī tad, ja kļūda atgadīsies, nosūtot 1002.pieprasījumu. Šajā gadījumā Tirgotājs saņem pieprasījumu sinhroni.

Gadījumā, ja pēc Klienta novirzīšanas uz maksājuma apstiprināšanas mājas lapu, Klients aizver web pārlūkprogrammu, neautorizējas vai neapstiprina maksājumu, Tirgotājs nesaņems atbildi.

Pēc maksājuma apstrādes Banka asinhroni nosūta 1102.pieprasījumu ar dažādām vērtībām VK_T_STATUS laukā:

- Pēc tam, kad Klients apstiprinājis maksājuma rīkojuma nosūtīšanu, tas tiek saglabāts DB, bet vēl nav apstrādāts Bankas sistēmā. Banka nosūta atbildi „1102" ar statusu „1";
- Pēc veiksmīgas maksājuma apstrādes Bankas sistēmā, Banka nosūta atbildi „1102" ar statusu „2" Tirgotājam;
- Ja Klients neapstiprina maksājuma rīkojumu vai kāda iemesla dēļ maksājuma rīkojums nevar tikt pieņemts izpildei (nepietiek līdzekļu Klienta kontā, u.c.), tad Banka nosūta atbildi „1102" ar statusu „3".

Tabula 2. 1102.pieprasījums „Maksājuma statuss"

Nr.	Parametrs	Piedalās elektr. parakstā	Maks. garums	Apraksts	Skaidrojums
1.	VK_SERVICE	Jā	4	Pieprasījuma tips (1102)	1102
2.	VK_VERSION	Jā	3	Elektroniskā paraksta algoritms (101)	101
3.	VK_SND_ID	Jā	20	Sūtītāja ID (bankas)	Veido banka
4.	VK_REC_ID	Jā	20	Saņēmēja ID (Tirgotāja)	VK_SND_ID lauks no 1002.pieprasījuma
5.	VK_STAMP	Jā	32	Pieprasījuma ID – unikāls numurs – (banka neizmanto)	VK_STAMP lauks no 1002. pieprasījuma
6.	VK_T_NO	Jā	12	Maksājuma rīkojuma numurs	Veido banka
7.	VK_AMOUNT	Jā	13	Maksājuma summa	VK_AMOUNT lauks no 1002. pieprasījuma
8.	VK_CURR	Jā	3	Maksājuma valūta (EUR)	EUR
9.	VK_REC_ACC	Jā	21	Saņēmēja konts	VK_ACC lauks no 1002. pieprasījuma
10.	VK_REC_NAME	Jā	105	Saņēmēja nosaukums	VK_NAME lauks no 1002. pieprasījuma
11.	VK_REC_REG_ID	Jā	20	Saņēmēja reģistrācijas numurs	VK_REG_ID lauks no 1002. pieprasījuma
12.	VK_REC_SWIFT	Jā	20	Saņēmēja bankas kods	VK_SWIFT lauks no 1002. pieprasījuma
13.	VK_SND_ACC	Jā	21	Maksātāja konts	Maksātāja konts
14.	VK_SND_NAME	Jā	105	Maksātāja vārds	Maksātāja vārds
15.	VK_REF	Jā	20	Maksājuma numurs pie Tirgotāja	VK_REF lauks no 1002. pieprasījuma
16.	VK_MSG	Jā	140	Maksājuma detaļas	VK_MSG lauks no 1002. pieprasījuma
17.	VK_T_DATE	Jā	10	Maksājuma apstrādes datums	Veido banka
18.	VK_T_STATUS	Jā	4	Maksājuma apstrādes statuss	1 – Pieņemts izpildei 2 – Izpildīts 3 – Atcelts
19.	VK_MAC	Nē	300	Elektroniskais paraksts	Veido banka

20.	VK_LANG	Nē	3	Vēlamā valoda (LAT/ENG/RUS)	LAT

4.2. Autorizācija ārējās sistēmās

4.2.1. 2001.pieprasījums „Klienta autorizācija ārējā sistēmā”

Banka novirza Klientu uz izvēlēto Tirgotāju / ārējo sistēmu ar parametriem, kas aprakstīti 2001.pieprasījumā. Šis pieprasījums tiek nosūtīts ar POST metodi uz izvēlētā Tirgotāja / ārējas sistēmas adresi, kas norādīta līgumā.

Tabula 3. 2001.pieprasījums „Klienta autorizācija ārējā sistēmā”

Nr.	Parametrs	Piedalās elektr. parakstā	Maks. garums	Apraksts	Skaidrojums
1.	VK_SERVICE	Jā	4	Pieprasījuma tips (2001)	2001
2.	VK_VERSION	Jā	3	Elektroniskā paraksta algoritms (101)	101
3.	VK_SND_ID	Jā	20	Sūtītāja ID (bankas)	Veido banka
4.	VK_REC_ID	Jā	20	Saņēmēja ID (tirgotājs/ārējā sistēma)	Lauks no līguma ar Tirgotāju (Tirgotāja identifikators)
5.	VK_STAMP	Jā	32	Pieprasījuma ID – unikālais numurs	VK_STAMP lauks no 3001.pieprasījuma, autorizācijas pēc bankas iniciatīvas gadījumā lauks ir tukšs
6.	VK_T_NO	Jā	12	Atbildes ID – unikālais numurs	Veido banka (katram pieprasījumam unikāls)
7.	VK_PER_CODE	Jā	12	Personas kods	Personas kods
8.	VK_PER_FNAME	Jā	100	Klienta vārds	-
9.	VK_PER_LNAME	Jā	100	Klienta uzvārds	-
10.	VK_COM_CODE	Jā	20	Uzņēmuma reģistrācijas numurs	-
11.	VK_COM_NAME	Jā	200	Uzņēmuma nosaukums	-
12.	VK_TIME	Jā	32	Pieprasījuma timestamp	Formāts yyyyMMddHHmmSS
13.	VK_MAC	Nē	300	Elektroniskais paraksts	Veido banka
14.	VK_LANG	Nē	3	Vēlamā valoda (LAT/ENG/RUS)	LAT

4.3. Klienta personīgo datu nosūtīšana Tirgotājam

4.3.1. 3001.pieprasījums „Pieprasījums pēc klienta datiem”

Šis pieprasījums ir nosūtīts ar POST metodi uz Bankas adresi, kas ir norādīta līgumā.

Tabula 4. 3001.pieprasījums „Pieprasījums pēc klienta datiem”

Nr.	Parametrs	Piedalās elektr. parakstā	Maks. garums	Apraksts	Skaidrojums
1.	VK_SERVICE	Jā	4	Pieprasījuma tips (3001)	3001
2.	VK_VERSION	Jā	3	Elektroniskā paraksta algoritms (101)	101
3.	VK_SND_ID	Jā	20	Tirgotāja/ārējās sistēmas ID	Tirgotāja identifikators
4.	VK_STAMP	Jā	32	Pieprasījuma ID – unikāls numurs	Veido tirgotājs (katram pieprasījumam unikāls)
5.	VK_RETURN	Jā	400	URL, kur novirzīt Klientu pēc procesa beigām	Veido tirgotājs
6.	VK_MAC	Nē	300	Elektroniskais paraksts	Veido tirgotājs
7.	VK_LANG	Nē	3	Vēlamā valoda (LAT/ENG/RUS)	LAT

4.3.2. 2001.pieprasījums „Klienta autorizācija ārējā sistēmā”

Gadījumā, ja Klients apstiprina datu nosūtīšanu Tirgotājam, Banka novirza Klientu uz izvēlēto Tirgotāja / ārējās sistēmas adresi ar parametriem, kas aprakstīti 2001.pieprasījumā. Šis pieprasījums tiek nosūtīts ar POST metodi uz adresi, kas norādīta 3001.pieprasījuma VK_RETURN parametrā.

5. Maksājumu apstrāde Bankas sistēmās

5.1. DNB Link moduļi

DNB Link “Maksājumu modulis” ir pieejams internetbankas Klienta (fiziskas personas) un Klienta (juridiskas personas) lietotājiem, ja attiecīgajam lietotājam noteiktās pilnvaras un paraksts atļauj maksājumu funkcionalitātes izmantošanu.

DNB Link “Autentifikācijas modulis” ir pieejams tikai fiziskām personām ar nosacījumu, ja internetbankas “lietotājs = klients”.

5.2. DNB Link maksājumu apstrāde internetbankā daudzlietotāju situācijās

Situācijās, kad DNB Link izmanto Klients - juridiska persona vai Klients – fiziska persona ar speciālām internetbankas izmantošanas tiesībām, DNB Link maksājuma apstrāde norit līdzīgi kā citu (piem., iekšzemes, starptautisko) internetbankas maksājumu apstrāde – tā izveidošana sākas DNB Link izmantošanas brīdī, bet tālākās aktivitātes norit lietotājiem ielogojoties internetbankā parastā veidā.

Ja kādas no internetbankas lietotājam noteiktajām pilnvarām (internetbankas izmantošanas režīms, paraksts, paraksta diapazona limits, dienas un maksājuma limits) nepieļauj internetbankas maksājuma noformēšanu un nosūtīšanu izpildei momentāni DNB Link izmantošanas brīdī, tad turpmākā maksājuma apstrāde notiek internetbankā no izvēlnes „BANKA – Maksājumi – Maksājumu saraksts”. Klients izvēlnē „Maksājumu saraksts” var veikt standarta darbības ar maksājumu, t.i., dzēst, rediģēt (tikai izmainīt maksātāja konta numuru), parakstīt un nosūtīt izpildei.

Daudzlietotāju situācijās ir īpaši jāievēro parametra VK_TIME_LIMIT ierobežojumi.

5.3. Internetbankas darba režīmi un maksājumu izpildes ierobežojumi

5.3.1. Darba režīms

Internetbanka strādā diennakts režīmā.

Internetbankas darbība var tikt ierobežota vai pārtraukta tehnisku pārtraukumu vai sistēmu profilakses veikšanai.

5.3.2. Maksājumu izpildes ierobežojumi

DNB Link maksājumā tiek izmantots parametrs VK_TIME_LIMIT.

VK_TIME_LIMIT ir „maksājuma derīguma termiņš" – laiks, līdz kuram maksājumu var parakstīt internetbankā (ar visiem nepieciešamajiem parakstiem) un izpildīt Bankas sistēmā. Maksājumā norādītajam VK_TIME_LIMIT ir jābūt „lielākam / vienādam" par tekošo sistēmas laiku, tad maksājumu ir iespējams veiksmīgi apstrādāt un izpildīt.

Līdz bankas turpmākajam rīkojumam parametrs VK_TIME_LIMIT ir jānorāda kā tukšs lauks. Tiks izmantots bankas parametrs pēc noklusējuma, tas ir, +10 dienas pulksten 21:00.

6. Bibliotēku apraksts

6.1. Mapju apraksts

Arhīvs satur šādas mapes:

- Data – satur skriptus, lai radītu 3001 un 2001 pieprasījumus un analizētu to atbildes;
- Shop – satur skriptus, lai radītu 1002 un 1102 pieprasījumus un analizētu to atbildes;
- Src – satur bibliotēku pirmkodus.

Saites uz bibliotēkām atrodas šeit:

https://www.dnb.lv/sites/default/files/corporate_remote_banking/documents/Java.zip
https://www.dnb.lv/sites/default/files/corporate_remote_banking/documents/net.zip
https://www.dnb.lv/sites/default/files/corporate_remote_banking/documents/php.zip

6.2. PHP un Java

6.2.1. Klase InordLink

Bāzes klase priekš klientu bibliotēku API. Tās metodes netiek izmantotas tieši.

6.2.2. Klase AuthorizationRequest

Klase ģenerē atbildi no Bankas priekš 2001 "Klienta autorizācija ārējā sistēmā" un 3001 "Klienta datu pieprasījums" pieprasījuma.

Metodes nosaukums	Apraksts
Constructor	Priekš inicializācijas tiek lietots galvenais konstruktors. Parametri ir pieminēti 3. tabulā. Papildus parametrs ir pPub – ceļš līdz bankas publiskajam PKCS#8 sertifikātam PEM formātā.
decode	Metode tiek lietota, lai pārbaudītu atbildes integritāti, lietojot v_mac parametru un atbilstošu šifrēšanas algoritmu.

6.2.3. Klase CustomerDataRequest

Klase Bankai ģenerē pieprasījumu priekš 3001 "Klienta datu pieprasījums" pieprasījuma.

Metodes nosaukums	Apraksts
Constructor	Priekš inicializācijas tiek lietots galvenais konstruktors. Parametri ir pieminēti 4. tabulā. Papildus parametrs ir pPriv – ceļš līdz lieltirgotāja privātajam PKCS#8 sertifikātam PEM formātā.

6.2.4. Klase OrderRequest

Klase Bankai ģenerē pieprasījumu priekš 1002 "Dati maksājuma rīkojumam" pieprasījuma.

Metodes nosaukums	Apraksts
Constructor	Priekš inicializācijas tiek lietots galvenais konstruktors. Parametri ir pieminēti 1. tabulā. Papildus parametrs ir pPriv – ceļš līdz lieltirgotāja privātajam PKCS#8 sertifikātam PEM formātā.

6.2.5. Klase OrderResponse

Klase ģenerē atbildi no Bankas 1102 "Maksājuma statuss" pieprasījumam.

Metodes nosaukums	Apraksts
Constructor	Priekš inicializācijas tiek lietots galvenais konstruktors. Parametri ir pieminēti 2. tabulā. Papildus parametrs ir pPub – ceļš līdz bankas publiskajam PKCS#8 sertifikātam PEM formātā.
decode	Metode tiek lietota, lai pārbaudītu atbildes integritāti, lietojot v_mac parametru un atbilstošu šifrēšanas algoritmu.

6.3. .NET

6.3.1. Klase InordLink

Bāzes klase priekš klientu bibliotēku API. Tās metodes netiek izmantotas tieši.

6.3.2. Klase AuthorizationRequest

Klase ģenerē atbildi no Bankas priekš 2001 "Klienta autorizācija ārējā sistēmā" un 3001 "Klienta datu pieprasījums" pieprasījuma.

Metodes nosaukums	Apraksts
Constructor	Priekš inicializācijas tiek lietots galvenais konstruktors. Parametri ir pieminēti 3. tabulā. Papildus parametrs ir pPub – ceļš līdz bankas publiskajam PKCS#8 sertifikātam PEM formātā.
decode	Metode tiek lietota, lai pārbaudītu atbildes integritāti, lietojot v_mac parametru un atbilstošu šifrēšanas algoritmu.

6.3.3. Klase CustomerDataRequest

Klase Bankai ģenerē pieprasījumu priekš 3001 "Klienta datu pieprasījums" pieprasījuma.

Metodes nosaukums	Apraksts
Constructor	Priekš inicializācijas tiek lietots galvenais konstruktors. Parametri ir pieminēti 4. tabulā. Papildus parametri ir : • pPriv – ceļš līdz lieltirgotāja privātajam PKCS#12 sertifikātam; • pPass – parole lieltirgotāja PKCS#12 sertifikātam.

6.3.4. Klase OrderRequest

Klase Bankai ģenerē pieprasījumu priekš 1002 "Dati maksājuma rīkojumam" pieprasījuma.

Metodes nosaukums	Apraksts

Constructor	Priekš inicializācijas tiek lietots galvenais konstruktors. Parametri ir pieminēti 1. tabulā. Papildus parametri ir : • pPriv – ceļš līdz lieltirgotāja privātajam PKCS#12 sertifikātam; • pPass – parole lieltirgotāja PKCS#12 sertifikātam.

6.3.5. Klase OrderResponse

Klase ģenerē atbildi no Bankas 1102 "Maksājuma statuss" pieprasījumam.

Metodes nosaukums	**Apraksts**
Constructor	Priekš inicializācijas tiek lietots galvenais konstruktors. Parametri ir pieminēti 2. tabulā. Papildus parametrs ir pPub – ceļš līdz bankas publiskajam PKCS#8 sertifikātam PEM formātā.
decode	Metode tiek lietota, lai pārbaudītu atbildes integritāti, lietojot v_mac parametru un atbilstošu šifrēšanas algoritmu.

7. Prasības pret Bankas nosaukumu un grafisko attēlu

Tirgotājs savā lapā izvieto Bankas grafisko attēlu un nosaukumu atbilstoši Bankas prasībām:

- Ir jāizmanto Bankas nosaukums – **DNB banka** (pievērsiet uzmanību lielajiem un mazajiem burtiem!);
- Ir jāizmanto Bankas grafiskais attēls, kas izvietots Bankas mājas lapā izvēlnē „Uzņēmumiem – Attālinātie pakalpojumi – DNB Link" (doti .gif un .eps formāti).