AUTENTIFIKAVIMO DUOMENŲ PERDAVIMO SPECIFIKACIJA

1. Techniniai autentifikavimo realizacijos reikalavimai

1.1. Banko reikalingų autentifikavimo duomenų integracija Paslaugos gavėjo Tinklalapyje(toliau – Svetainėje).

Banko autentifikavimo sistema turi būti užregistruota Svetainėje su tokiais parametrais:

1. Pradinio autentifikavimo puslapio interneto adresu (URL). Į šį adresą bus persiunčiama autentifikavimo procedūros inicijavimo komanda su nuoroda į šaltinį – Svetainę. Tuomet Banko sistemoje po sėkmingo autentifikavimo turi būti realizuotas automatinis atgalinis peradresavimas ir autentifikavimo paketo grąžinimas į Svetainę;
2. Banko viešu raktu.

Banko autentifikavimo sistemoje turi būti užregistruotas ir naudojamas Paslaugos gavėjo Svetainės puslapio interneto adresas (URL), į kurį nukreipiamas Naudotojas, sėkmingai praėjęs autentifikavimo procedūrą ir į kurį nusiunčiamas autentifikavimo paketas.

Banko svetainės serverių laikrodžiai turi būti sinchronizuojami su interneto atominiais laikrodžiais, nes vienas iš autentifikavimo paketo parametrų yra tikslus autentifikavimo laikas. Toks pat reikalavimas galioja ir Paslaugos gavėjo Svetainės serveriams.

Banko svetainėje turi būti realizuotos autentifikavimo paketų formavimo ir nukreipimo į Svetainę priemonės pagal žemiau išdėstytus techninius reikalavimus.

Normaliame darbo režime, Banko svetainės puslapiuose turi būti nuorodos, meniu arba kiti valdymo elementai, kurių pagalba sėkmingai autentifikuotas Banko sistemoje Naudotojas galėtų interaktyviai inicijuoti perėjimą į Svetainę be pakartotino autentifikavimo.

1.2. Integruoto autentifikavimo procesas

Autentifikavimo duomenų perdavimas realizuojamas „Server - Client – Server “principu, kuomet persijungimai tarp Svetainių ir autentifikavimo paketų fiziškai realizuojami per interneto naršyklę Naudotojo įrenginyje, nors inicijuojami ir transportuojami duomenys generuojami Paslaugos gavėjo ir Banko svetainių serveriuose.

1.3. Autentifikavimo scenarijai

Integruotas autentifikavimas vyksta 2 būdais:

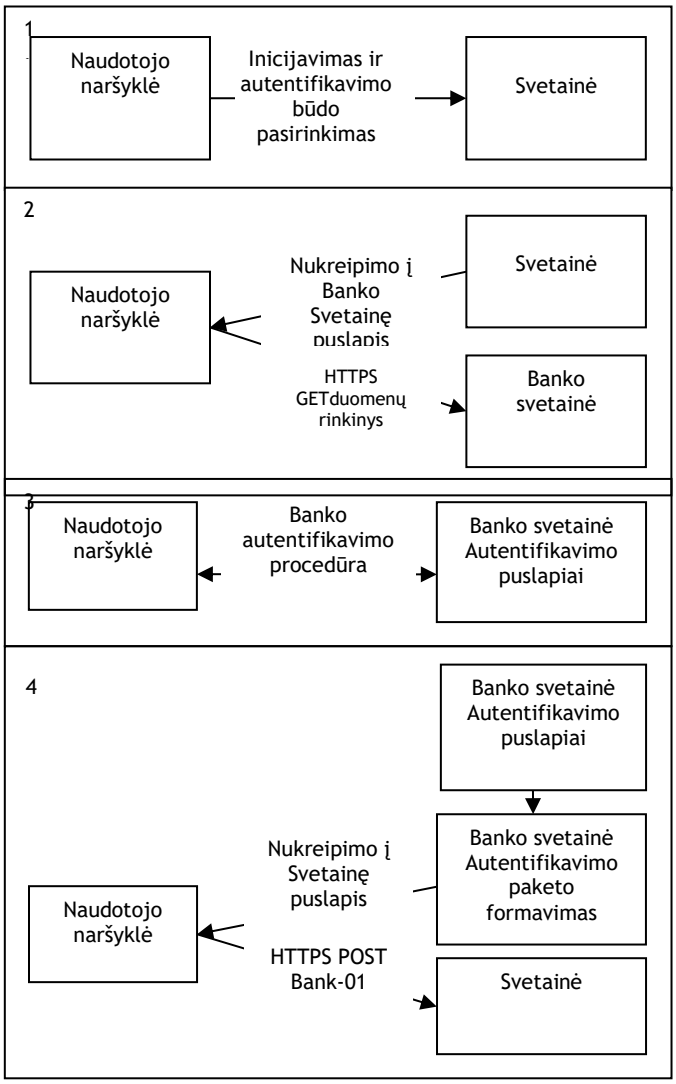
1. Naudotojas pradeda darbo seansą Svetainėje;
2. Naudotojas pradeda darbo seansą Banko svetainėje.

Toliau abu scenarijai aprašomi detaliau.

1.3.1. Naudotojas pradeda darbo seansą Svetainėje (*Pav. 1 Seanso inicijavimas Svetainėje*):

1. Naudotojas pradėjo darbą Svetainėje, pasirenka norimą banką pagal iš anksto užregistruotų bankų sąrašą ir paspaudžia autentifikavimo pradžios mygtuką;
2. Naudotojas nukreipiamas į banko svetainės autentifikavimo puslapį su HTTPS GET parametru, identifikuojančiu į kokią sistemą norima jungtis.
3. Naudotojas Banko svetainėje autentifikuojasi standartiškai (įprastai);

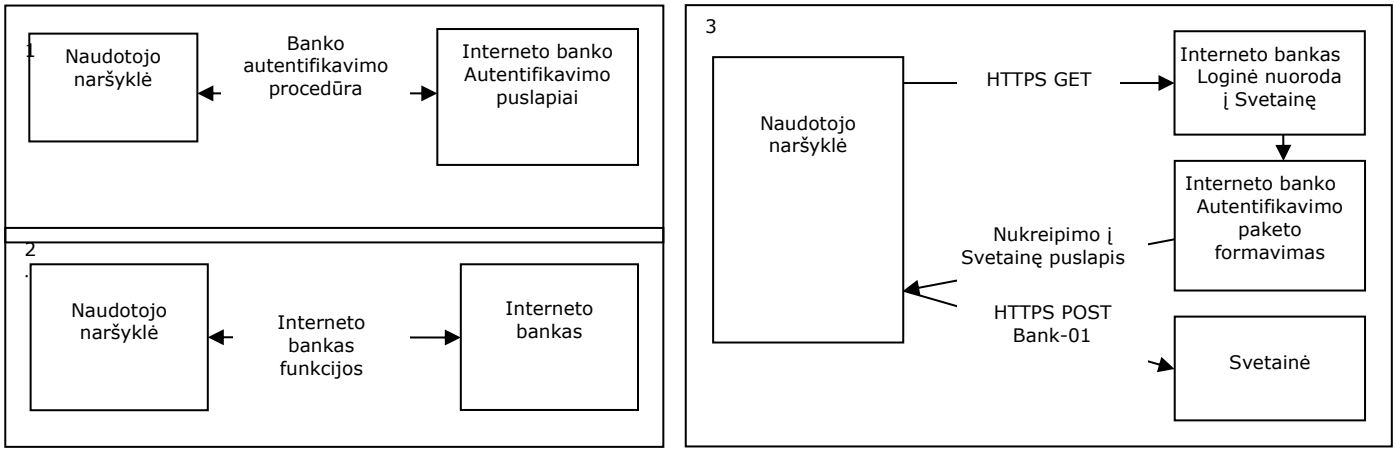
4. Sėkmingai identifikavus Naudotoją, Banko svetainėje suformuojamas autentifikavimo paketas ir inicijuojamas peradresavimas į Svetainę, persiunčiant autentifikavimo duomenis HTTPS POST metodu (duomenų rinkinys BANK-01).



Pav. 1 Seanso inicijavimas Svetainėje

1.3.2. Naudotojas pradeda darbo seansą Banko interneto banke (*Pav. 2 Seanso inicijavimas interneto banke*):

1. Naudotojas iš karto pradeda darbo seansą Banko interneto banke ir praeina įprastą autentifikavimo procedūrą;
2. Naudotojas vykdo interneto banke norimas funkcijas;
3. Numatytame interneto banko skyriuje naudotojas pasirenka perėjimą prie Svetainės ir paspaudžia atitinkamą mygtuką. Tuomet interneto banke suformuojamas autentifikavimo paketas ir automatiškai inicijuojamas peradresavimas į Svetainę, persiunčiant autentifikavimo duomenimis HTTPS POST metodu (duomenų rinkinys BANK-01).



Pav. 2 Seanso inicijavimas interneto banke

2. Autentifikavimo duomenys

2.1 Fizinių asmenų

Banko sistemoje turi būti nustatomi ir perduodami Svetainei tokie Naudotojo autentifikavimo duomenys:

1. Naudotojo autentifikavimo Banko sistemoje einamasis laikas sekundės tikslumu;
2. Fizinio asmens kodas;
3. Fizinio asmens vardas;
4. Fizinio asmens pavardė.

2.2 Juridinių asmenų

Banko sistemoje turi būti nustatomi ir perduodami Svetainei tokie Naudotojo autentifikavimo duomenys:

1. Naudotojo autentifikavimo Banko sistemoje einamasis laikas sekundės tikslumu;
2. Juridinio asmens atstovo asmens kodas;
3. Juridinio asmens atstovo asmens vardas;
4. Juridinio asmens atstovo asmens pavardė;
5. Juridinio asmens kodas;
6. Juridinio asmens pavadinimas.

Tekstiniai paketo duomenys pateikiami standartinėje *UTF-8 koduotėje*.
Autentifikavimo duomenys perduodami Svetainei atskiruose paketo BANK-01 parametruose.

3. Saugumas

3.1. Duomenų transportavimo saugumas

Duomenų transportavimo saugumas užtikrinamas HTTPS protokolu, kuriuo vyksta duomenų apsikeitimas, kaip nukreipiant Naudotoją tarp Svetainės ir Banko svetainių, taip ir tų svetainių viduje.

3.2. Autentifikavimo duomenų pasirašymas

Autentifikavimo duomenys pasirašomi Banko sertifikato privačiu raktu, pritaikant algoritmą **RSASSA-PKCS1-v1_5** su **SHA-1** HASH-funkcija.

Banko viešo rakto sertifikatas, naudojamas parašo kontrolei, turi būti perduotas Paslaugos gavėjui ir užregistruotas Svetainės galutinės sutarties sudarymo momentu.

Skaitmeninis parašas turi būti išskaičiuojamas tekstinei eilutei, sudarytai iš visų autentifikavimo duomenų parametrų.

Fizinių asmenų: *SRC* || *TIME* || *PERSON_CODE* || *PERSON_FNAME* || *PERSON_LNAME*

Juridinių asmenų: *SRC* || *TIME* || *PERSON_CODE* || *PERSON_FNAME* || *PERSON_LNAME* || *COMPANY_CODE* || *COMPANY_NAME*

Čia || - yra tekstinių eilučių apjungimo operacija, o ne skiriamieji simboliai. Parametrų vardai pateikti pagal paketą BANK-01.
Išskaičiuotas skaitmeninis parašas turi būti perduodamas Svetainei atskirame paketo BANK-01 parametre.

Fiziniai asmenys

Iš Svetainės į Banko svetainės autentifikavimo puslapį patenkama HTTPS GET metodu adresu
https://e.sb.lt/authorization/login?system=
(nurodyti, svetainės adresą ar įmonės vardą, pvz. system=IMONE)

BANK-01

Šis parametrų duomenų rinkinys siunčiamas HTTPS POST metodu iš Banko svetainės į Svetainės autentifikavimo puslapį adresu: **[statinis Callback URL]**

Duomenų rinkinio parametrų struktūra:

Parametras	Maksimalus ilgis	Paskirtis
SRC	20	Užklausos šaltinio kodas – **Banko kodas**
TIME	20	Naudotojo nukreipimo iš Svetainės į Banko svetainę data ir laikas sekundžių tikslumu. Data perduodama tekstiniame pavidale formate ***YYYY.MM.DD hh:mm:ss***
PERSON_CODE	20	Asmens kodas
PERSON_FNAME	100	Asmens vardas
PERSON_LNAME	100	Asmens pavardė
SIGNATURE	300	Autentifikavimo duomenų skaitmeninis Banko parašas, konvertuotas į BASE64 formatą. Parašas išskaičiuojamas pagal algoritmą, aprašytą *3.2. Autentifikavimo duomenų pasirašymas*
TYPE	10	Užklausos tipas. Fiksuota reikšmė: *BANK-01*

Juridiniai asmenys

Iš Svetainės į Banko svetainės autentifikavimo puslapį patenkama HTTPS GET metodu adresu
https://e.sb.lt/authorization/login?system=
(nurodyti, svetainės adresą ar įmonės vardą, pvz. system=IMONE)

BANK-01

Šis parametrų duomenų rinkinys siunčiamas HTTPS POST metodu iš Banko svetainės į Svetainės autentifikavimo puslapį adresu: **[statinis Callback URL]**

Duomenų rinkinio parametrų struktūra:

Parametras	Maksimalus ilgis	Paskirtis
SRC	20	Užklausos šaltinio kodas – **Banko kodas**
TIME	20	Naudotojo nukreipimo iš Svetainės į Banko svetainę data ir laikas sekundžių tikslumu. Data perduodama tekstiniame pavidale formate ***YYYY.MM.DD hh:mm:ss***
PERSON_CODE	20	Asmens kodas
PERSON_FNAME	100	Asmens vardas
PERSON_LNAME	100	Asmens pavardė
COMPANY_NAME	200	Juridinio asmens pavadinimas (neprivalomas)
COMPANY_CODE	20	Juridinio asmens kodas (neprivalomas)
SIGNATURE	300	Autentifikavimo duomenų skaitmeninis Banko parašas, konvertuotas į BASE64 formatą. Parašas išskaičiuojamas pagal algoritmą, aprašytą *3.2. Autentifikavimo duomenų pasirašymas*
TYPE	10	Užklausos tipas. Fiksuota reikšmė: *BANK-01*