



Wstęp

API łączące system **Brama** z systemem **obsługi szlabanów** jest jednokierunkowe.

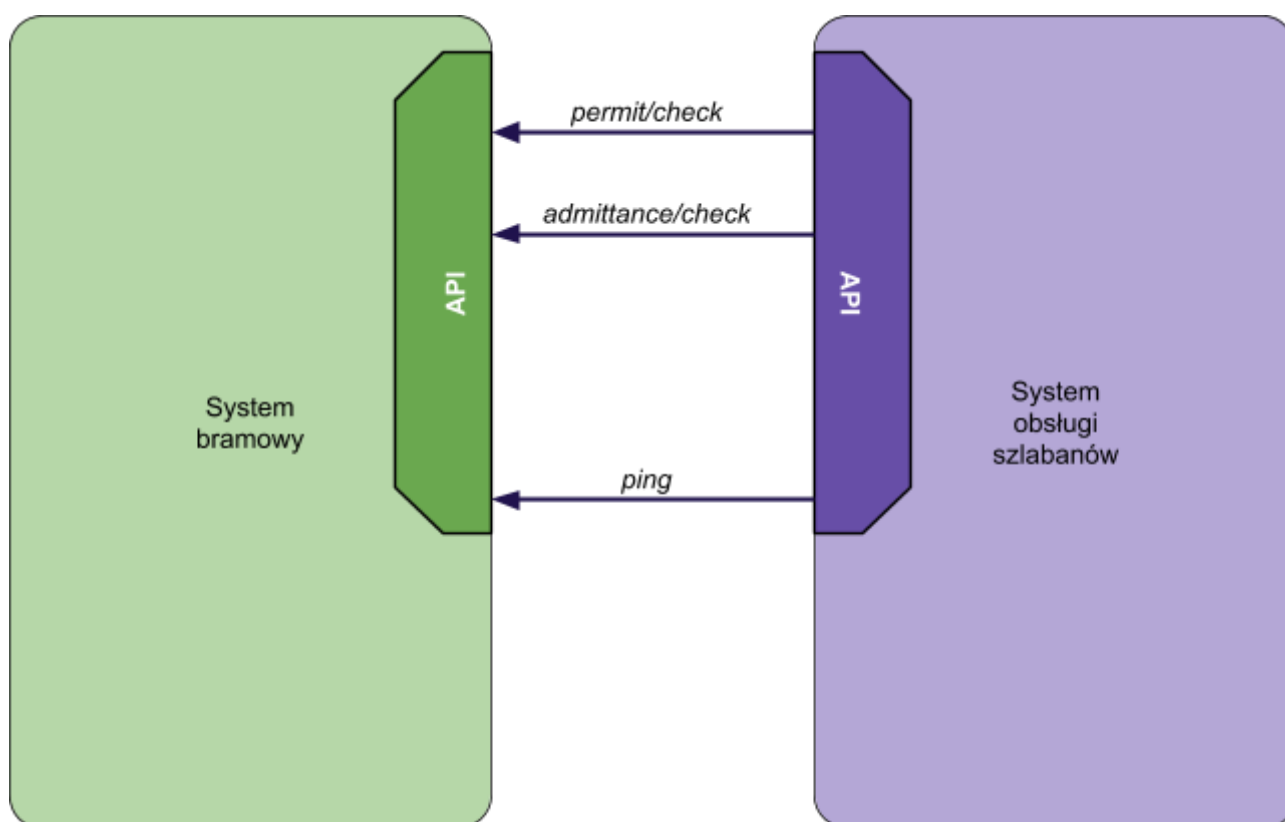
Głównym celem API jest **weryfikacja na rzecz systemu obsługi szlabanów** ważności kart dostępowych i przepustek jednorazowych uprawniających do wstępu na wybrane tereny Portu.

Dodatkowym celem jest **zbieranie w systemie bramowym informacji** o ruchu użytkowników.

Każdy z systemów przechowuje dane na własne potrzeby i pozwala na zarządzanie nimi.

Komunikacja między systemami odbywa się w przypadku zajścia zdefiniowanych określonych zdarzeń.

Schemat systemów





Informacje techniczne

Dane w API przesyłane są poprzez HTTP POST, nazwy parametrów są pisane małymi literami.

Przy opisie poszczególnych poleceń, parametr [URL](#) dla API jest równy:

- <https://brama.port.szczecin.pl> - dla środowiska produkcyjnego,
- <http://staging.brama.port.szczecin.pl> - dla środowiska testowego,

Format odpowiedzi to XML lub JSON, kodowanie UTF-8.

Nagłówki XML odpowiedzi wygląda następująco:

```
<?xml version="1.0" encoding="UTF-8" ?>
```

Daty zapisane są w strefie czasowej UTC i w formacie: YYYY-MM-DD HH:MM:SS

lub YYYY-MM-DD HH:MM

Długość pól typu STRING jest podana w nawiasach - np. STRING (45).

Dopuszczalna częstotliwość wywoływania metod API to 1/sekundę, natomiast niektóre metody mogą mieć dodatkowe ograniczenia.

Identyfikatory obszarów i bram są konfigurowane przez PORT.

W API należy używać cudzysłowów prostych.

Pod adresem [URL/api/transport/demo](#) znajduje się strona pozwalająca na przeprowadzenie testów API – wysyłanie poleceń na serwer i obserwowanie odpowiedzi.

Obowiązkowe nagłówki protokołu HTTP:

- Accept: application/xml
(jeśli oczekiwana jest odpowiedź w formacie XML)
- Accept: application/json
(jeśli oczekiwana jest odpowiedź w formacie JSON - nie dotyczy wszystkich metod API)
- API-Version: YYYY-MM-DD
(należy użyć daty z nagłówka/stopki tego dokumentu)



Przepustki i karty dostępowe

Przepustki jednorazowe są kwitami wydawanymi na stanowiskach bramowych, zwykle na podstawie wcześniejszej awizacji (zapowiedzi). Zawierają wydrukowany na drukarce termicznej kod kreskowy ze swoim identyfikatorem. Mają z założenia krótki termin ważności. Mogą mieć ważność ograniczoną do wybranego obszaru Portu. Ich identyfikator ma postać /P1234567 (tj. prefiks /P i 7 cyfr dziesiętnych)

Karty dostępowe to karty MIFARE z nadrukiem identyfikującym osobę (pojazd), dla której je wydano i wskazującym na zakres uprawnień (np. do wprowadzania gości). Obowiązują na wskazanych terenach dostępowych (nie są identyczne z obszarami portu). Ich identyfikator jest zapisany elektronicznie na karcie dostępowej i ma postać 8 cyfr szesnastkowych (np. ABCD1234)

Tereny dostępowe

Zakresy dostępu przekazywane są w postaci ciągu znaków zawierającego po przecinku oznaczenia według tabeli terenów (w dalszej części dokumentu).

Ciąg nie powinien zawierać cudzysłowów. Ciąg może opcjonalnie zawierać spację po przecinkach. Przykładowo ciąg „B, D” oznacza dostęp do terenu „Bulk Cargo” i terenu „Łasztownia”). Pusty ciąg oznacza całkowity brak dostępu.

Tabela terenów dostępowych:

	Oznaczenia terenów dostępowych
„A”	Cały teren ZMPSiŚ S.A. (bez terminala promowego w Świnoujściu)
„B”	Teren „Bulk Cargo”
„D”	Teren „Łasztownia”
„WOC”	Teren Wolnego Obszaru Celnego
„T”	Teren nabrzeża „Warsztatowe”
„H”	Teren nabrzeża „HUK”
„S”	Teren portu handlowego w Świnoujściu (bez nabrzeża „Portowców”)
„P”	Teren nabrzeża „Portowców”
„F”	Teren terminala promowego w Świnoujściu



Komunikaty o błędach

Informacja o błędzie uwierzytelniania przekazywana jest w kodzie HTTP 403 i parametrach wyjściowych:

```
{
  "errorCode": "AUTH_FAIL",
  "errorMessage": "Authentication failure"
}
```

Błędy walidacji danych będą przekazywane w formacie:

```
{
  "errorCode": "VALIDATION_ERROR",
  "errorMessage": "Fields contain invalid data",
  "invalidFields": {
    "validUntil": "date value is in the past",
    "expiresOn": "string is not a valid date" //, ...
  }
}
```

Limit na częstotliwość wywoływania metod API wynosi 1/s.



Metody API

Sprawdzenie ważności przepustki jednorazowej

[URL](#)/api/permit/check

Parametry wejściowe:

- *user* - string - nazwa użytkownika API,
- *password* - string - hasło użytkownika API,
- *permitCode* - string - numer odczytany z kodu kreskowego przepustki (/P1234567),
- *locationCode* - string - identyfikator stanowiska z czytnikiem (w systemie zewnętrznym),
- *areald* - identyfikator obszaru portu, dla którego jest weryfikowana przepustka.

Odpowiedź JSON w przypadku powodzenia:

```
{
  "valid": true,
  "permitCode": string,
  "validUntil": string // date time
}
```

Odpowiedź JSON w przypadku braku dostępu:

```
{
  "valid": false,
  "permitCode": string,
  "error": string
}
```

Parametry wyjściowe:

- *valid* - parametr określający ważność przepustki jednorazowej;
- *validUntil* - date/time string - termin ważności przepustki zapisany w systemie bramowym;
- *error* - opcjonalny parametr z wyjaśnieniem braku dostępu w języku angielskim (np. karta jest jeszcze ważna, ale nie ma uprawnień do danego obszaru itp.)



Sprawdzenie ważności karty dostępowej

[URL](#)/api/admittance/check

Parametry wejściowe:

- *user* - string - nazwa użytkownika API,
- *password* - string - hasło użytkownika API,
- *mifareId* - string - numer seryjny karty (ABCD1234),
- *admittanceTo* - area string - oczekiwane tereny dostępowe karty,
- *locationCode* - string - identyfikator stanowiska z czytnikiem (w systemie zewnętrznym),

Odpowiedź JSON w przypadku powodzenia:

```
{
  "valid": true,
  "mifareId": string,
  "validUntil": string // date time
}
```

Odpowiedź JSON w przypadku braku dostępu:

```
{
  "valid": false,
  "mifareId": string,
  "error": string
}
```

Parametry wyjściowe:

- *valid* - parametr określający ważność przepustki jednorazowej;
- *mifareId* - string - numer seryjny karty (w celu potwierdzenia),
- *validUntil* - date/time string - miękki termin ważności karty zapisany w systemie bramowym.
- *error* - opcjonalny parametr z wyjaśnieniem braku dostępu w języku angielskim (np. karta jest jeszcze ważna, ale nie ma uprawnień do danego obszaru itp.)



Testowanie poprawności połączenia z systemem bramowym

[URL](#)/api/ping

Parametry wejściowe:

- *user* - string - nazwa użytkownika API,
- *password* - string - hasło użytkownika API,
- *sentAt* - date/time string - bieżący czas na serwerze obsługi szlabanów.

Odpowiedź JSON:

```
{
    "receivedAt": string
}
```

Parametry wyjściowe:

- *receivedAt* - date/time string - bieżący czas na serwerze bramowym.