

Tesi - Payment Request API

Daniele Rigon - 857319

31 luglio 2018

Indice

1	Overview Payment Request	2
1.1	Vantaggi	2
1.2	Come funziona	2
1.3	Uso API	3
1.3.1	Ruolo dell'utente	3
1.3.2	Ruolo del commerciante	3
1.3.3	Ruolo del browser	3
1.3.4	Metodi di pagamento	3
1.3.5	App di pagamento	4
1.3.6	Differenze tra metodo di pagamento e app di pagamento	4
2	Specifiche	5
2.1	Metodi	5
2.1.1	PaymentMethodData	5
2.1.2	PaymentDetails	5
2.1.3	PaymentOptions	7
2.1.4	PaymentRequest	7
3	Rischi e sicurezza	8
3.1	Esempio di un possibile attacco	8
3.1.1	Descrizione dell'attacco	8
3.1.2	Come difendersi	8
4	Implementazione PaymentRequest API su una pagina d'esempio	9
4.1	Costruttore	9
4.2	Visualizzazione dell'interfaccia utente, elaborazione del pagamento e visualizzazione dei risultati	9
4.3	Ascoltare gli eventi	13
5	Compatibilità web	14
6	Conclusioni	15

1 Overview Payment Request

La PaymentRequest API nasce con l'intento di creare esperienze di pagamento semplificate, in quanto ogni sito web ha il proprio sistema di pagamento e molti siti richiedono la ridigitazione manuale delle stesse informazioni più volte, le quali possono essere invece memorizzate e riutilizzate dall'API per completare più rapidamente le transazioni online.

1.1 Vantaggi

- **Esperienza di acquisto rapida:** gli utenti immettono i propri dati una sola volta nel browser, e dopo averli inseriti non è più necessario reinserirli su siti diversi;
- **Esperienza coerente su ogni sito che supporta l'API:** poiché la pagina di pagamento è controllata dal browser si può personalizzare l'esperienza utente, ad esempio includendo la localizzazione per impostare automaticamente la lingua preferita dell'utente o altre features;
- **Gestione delle credenziali:** gli utenti possono gestire le loro carte di credito e gli indirizzi di spedizione direttamente nel browser. Un browser può anche sincronizzare queste "credenziali" tra dispositivi, rendendo più semplice per gli utenti passare dal desktop al cellulare e viceversa quando si acquistano oggetti;
- **Gestione coerente degli errori:** il browser può controllare la validità dei numeri delle carte e può comunicare all'utente se una carta è scaduta o sta per scadere, può suggerire automaticamente quale carta utilizzare in base ai modelli di utilizzo passati o alle restrizioni del commerciante, o consentire all'utente di dire quale sia la carta predefinita/preferita;
- **Esperienza utente migliorata:** meno tipizzazione, coerenza tra i siti Web, tra browser e sistemi operativi e nuove funzionalità del browser per semplificare il checkout, ecc;
- **Miglioramento della sicurezza:** la PaymentRequest API ha il potenziale per ridurre le opportunità di frode e può facilitare l'adozione di metodi di pagamento più sicuri. Purtroppo ci sono dei problemi di sicurezza analizzati al capitolo 4;
- **Responsabilità inferiore:** in passato, per creare un'esperienza utente semplificata, i commercianti dovevano memorizzare le credenziali di pagamento degli utenti. Questo non è più necessario, il che può aiutare a ridurre la responsabilità del commerciante nei confronti del cliente.

1.2 Come funziona

La PaymentRequest API consente a un utente di completare una transazione più facilmente riutilizzando le informazioni memorizzate nel browser o in app di pagamento di terze parti. Quando l'utente preme un pulsante in una pagina di checkout collegata all'API il commerciante utilizza l'API per richiedere il pagamento. Il commerciante fornisce informazioni su prezzo, valuta e un elenco di metodi di pagamento accettati, e può inoltre richiedere al browser di creare un'interfaccia utente semplificata per raccogliere l'indirizzo di spedizione, le informazioni di contatto e altri elementi all'utente. Il browser determina quali metodi di pagamento sono supportati dal commerciante tra le varie "app di pagamento" mostrandole all'utente. L'utente seleziona un'app di pagamento con la quale pagare, la quale può comportare ulteriori interazioni con l'utente (ad esempio per l'autenticazione). Al completamento l'app di pagamento restituisce i dati tramite l'API al commerciante.

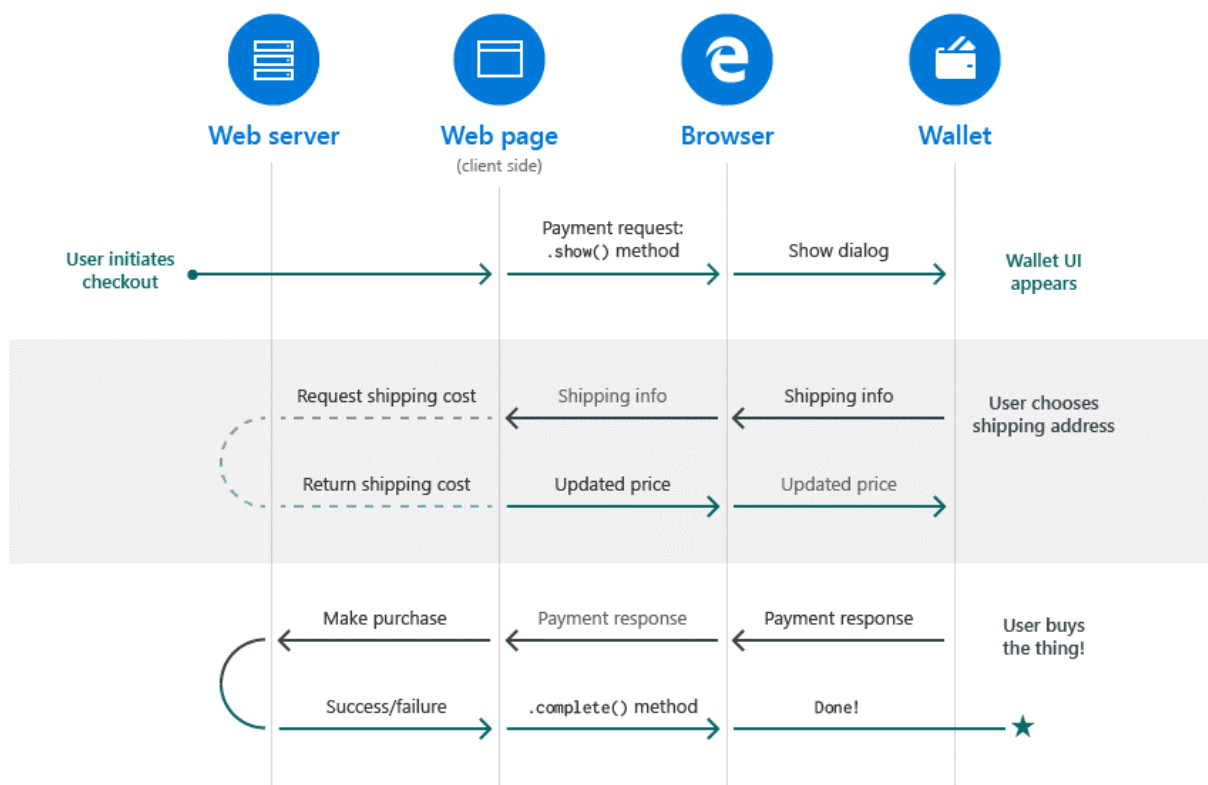


Figura 1: Schema Payment Request API

1.3 Uso API

1.3.1 Ruolo dell'utente

Gli utenti beneficiano del riutilizzo delle credenziali inserite nel browser o nelle app di pagamento. Quindi, quando si visita un sito Web che sfrutta la PaymentRequest API gli utenti avranno l'opportunità di sfruttare il riutilizzo semplificato delle credenziali archiviate.

1.3.2 Ruolo del commerciante

L'API influisce sul front end (l'interfaccia dell'esperienza utente) e non sul back-end, pertanto il commerciante non dovrebbe dover apportare modifiche all'elaborazione back-end dei vari metodi di pagamento; questo sarà compito del fornitore della pagina di pagamento il quale sostituirà i moduli Web con le chiamate alla PaymentRequest API.

1.3.3 Ruolo del browser

Il browser svolge diversi ruoli:

- Calcola l'intersezione dei metodi di pagamento accettati dal commerciante e registrati dall'utente;
- Visualizza l'interfaccia utente che consente all'utente di inserire le proprie informazioni;
- Funge da canale per i dati da e verso il commerciante e da e verso l'utente.

1.3.4 Metodi di pagamento

La PaymentRequest API è progettata per funzionare con un gran numero di metodi di pagamento, i quali vengono identificati attraverso due strade:

- I metodi di pagamento definiti da W3C sono identificati come "basic-card" e sono composti da stringhe corte;
- I metodi di pagamento definiti da altre parti sono identificati dagli URL.

1.3.5 App di pagamento

La PaymentRequest API, ovvero il browser, determina se un'app di pagamento "corrisponde" a una determinata transazione definendo un algoritmo che considera i metodi di pagamento accettati dal commerciante, dichiarati attraverso un elenco di identificativi del metodo di pagamento, passati attraverso l'API. Al fine di proteggere la privacy degli utenti i commercianti hanno accesso a informazioni molto limitate dell'utente.

Vediamo in che modo la PaymentRequest API influisce sul flusso dei metodi di pagamento che già supporta. Il normale flusso per gli utenti di solito implica qualcosa del genere:

- Scansione di un elenco di metodi di pagamento accettati;
- Scelta di un metodo;
- Per i metodi di pagamento che prevedono il lancio di un'app o la visita a un sito Web si invia l'utente a quell'app o sito;
- Pagamento completato.

La PaymentRequest API consente un flusso migliorato:

- L'utente preme un pulsante di acquisto singolo;
- Il browser visualizza le app di pagamento dell'utente che possono essere utilizzate per la transazione, ed è probabile che i browser supportino le preferenze dell'utente in modo che un'app di pagamento venga avviata automaticamente su un determinato sito Web, semplificando il checkout.
- Per i metodi di pagamento che prevedono il lancio di un'app o la visita a un sito Web, inviare l'utente a quell'app o sito;
- Pagamento completato;

1.3.6 Differenze tra metodo di pagamento e app di pagamento

Un'app di pagamento è il software che l'utente utilizza per pagare, la quale può supportare uno o più metodi di pagamento e può essere implementata utilizzando diverse tecnologie. I browser possono anche fungere da app di pagamento, memorizzando le credenziali dell'utente. In generale più app di pagamento possono implementare lo stesso metodo di pagamento. Vi sono casi importanti in cui è disponibile una sola app di pagamento autorizzata a supportare un metodo di pagamento, mentre ci sono casi in cui più app di pagamento possono servire diversi metodi di pagamento. In questo caso non è il commerciante che deve preoccuparsi dell'integrazione software, ma deve solamente richiedere le informazioni attraverso la PaymentRequest API.

2 Specifiche

2.1 Metodi

Per utilizzare l'API lo sviluppatore deve fornire e tenere traccia di una serie di informazioni chiave, le quali vengono passate al costruttore `PaymentRequest` come argomenti e successivamente utilizzate per aggiornare la richiesta di pagamento visualizzata all'utente. Queste informazioni sono:

- **PaymentMethodData:** rappresenta i metodi di pagamento che il sito supporta;
- **PaymentDetails:** rappresenta i dettagli della transazione. Ciò include il costo totale e facoltativamente un elenco di beni o servizi acquistati, beni materiali, opzioni di spedizione o "modificatori" su come vengono effettuati i pagamenti: ad esempio "se paghi con una carta di credito di tipo X incorre in una tassa di elaborazione di tot";
- **PaymentOptions:** il `PaymentOptions` viene passato al costruttore `PaymentRequest` e fornisce informazioni sulla consegna del prodotto: ad esempio per i beni fisici il commerciante avrà bisogno di un indirizzo fisico dove spedire, mentre per i beni digitali è sufficiente un'e-mail. Una volta che il `PaymentRequest` è stato costruito viene presentato all'utente finale tramite il metodo `show()`, il quale ritorna una promise che, una volta che l'utente conferma la richiesta di pagamento, si traduce in una `PaymentResponse`;
- **PaymentRequest:** la `PaymentRequest` serve a effettuare una richiesta di pagamento, in genere associata all'avvio di un processo di pagamento da parte dell'utente. La `PaymentRequest` consente agli sviluppatori di scambiare informazioni con l'user agent mentre l'utente sta fornendo dati in input. Poiché la visualizzazione simultanea di più interfacce `PaymentRequest` potrebbe confondere l'utente, questa specifica limita lo user agent a visualizzarne uno alla volta tramite il metodo `show()`;
- **PaymentDetailsInit:** Il `PaymentDetailsInit` viene utilizzato nella costruzione della richiesta di pagamento;
- **PaymentResponse:** un `PaymentResponse` viene restituito quando un utente ha selezionato un metodo di pagamento e approvato una richiesta di pagamento.

2.1.1 PaymentMethodData

`PaymentMethodData` contiene gli identificativi dei metodi di pagamento accettati dal sito Web e qualsiasi dato specifico del metodo di pagamento associato.

```
1  const methodData = [  
2    {  
3      supportedMethods: "basic-card",  
4      data: {  
5        supportedNetworks: ["visa", "mastercard"],  
6        supportedTypes: ["debit", "credit"],  
7      },  
8    },  
9    {  
10     supportedMethods: "https://example.com/bobpay",  
11     data: {  
12       merchantIdentifier: "XXXX",  
13       bobPaySpecificField: true,  
14     },  
15   },  
16 ];  
17
```

2.1.2 PaymentDetails

I details contengono informazioni sulla transazione che l'utente è invitato a completare.

```

1  const details = {
2    id: "super-store-order-123-12312",
3    displayItems: [
4      {
5        label: "Sub-total",
6        amount: { currency: "USD", value: "55.00" },
7      },
8      {
9        label: "Sales Tax",
10       amount: { currency: "USD", value: "5.00" },
11       type: "tax"
12     },
13   ],
14   total: {
15     label: "Total due",
16     // The total is USD$65.00 here because we need to
17     // add shipping (below). The selected shipping
18     // costs USD$5.00.
19     amount: { currency: "USD", value: "65.00" },
20   },
21 };
22

```

Opzioni di spedizione

Qui vediamo un esempio di come aggiungere due opzioni di spedizione ai details.

```

1  const shippingOptions = [
2    {
3      id: "standard",
4      label: "Ground Shipping (2 days)",
5      amount: { currency: "USD", value: "5.00" },
6      selected: true,
7    },
8    {
9      id: "drone",
10     label: "Drone Express (2 hours)",
11     amount: { currency: "USD", value: "25.00" }
12   },
13 ];
14 Object.assign(details, { shippingOptions });
15

```

Modifiche condizionali alla richiesta di pagamento

Qui vediamo come aggiungere una tassa di elaborazione per l'utilizzo di una carta di credito. Si noti che richiede il ricalcolo del totale.

```

1  // Credit card incurs a $3.00 processing fee.
2  const creditCardFee = {
3    label: "Credit card processing fee",
4    amount: { currency: "USD", value: "3.00" },
5  };
6
7  // Modifiers apply when the user chooses to pay with
8  // a credit card.
9  const modifiers = [
10   {
11     additionalDisplayItems: [creditCardFee],
12     supportedMethods: "basic-card",
13     total: {
14       {
15         label: "Total due",
16         amount: { currency: "USD", value: "68.00" },
17       },
18       data: {
19         {
20           supportedTypes: "credit",

```

```

21     },
22   },
23 ];
24 Object.assign(details, { modifiers });
25

```

2.1.3 PaymentOptions

Options contiene informazioni che lo sviluppatore ha bisogno dall'utente per eseguire il pagamento.

```

1   const options = {
2     requestPayerEmail: false,
3     requestPayerName: true,
4     requestPayerPhone: false,
5     requestShipping: true,
6   }
7

```

2.1.4 PaymentRequest

Dopo aver raccolto tutti i bit di informazioni prerequisite, ora possiamo costruirne uno PaymentRequest e richiedere che il browser lo presenti all'utente.

```

1   async function doPaymentRequest()
2   {
3     try
4     {
5       const request = new PaymentRequest(methodData, details, options);
6       // See below for a detailed example of handling these events
7       request.onshippingaddresschange = ev => ev.updateWith(details);
8       request.onshippingoptionchange = ev => ev.updateWith(details);
9       const response = await request.show();
10      await validateResponse(response);
11    } catch (err)
12    {
13      // AbortError, SecurityError
14      console.error(err);
15    }
16  }
17  async function validateResponse(response)
18  {
19    try {
20      if (await checkAllValuesAreGood(response))
21      {
22        await response.complete("success");
23      }
24      else {
25        await response.complete("fail");
26      }
27    } catch (err)
28    {
29      // Something went wrong...
30      await response.complete("fail");
31    }
32  }
33  doPaymentRequest();
34

```

3 Rischi e sicurezza

La PaymentRequest API aumenta la sicurezza poichè:

- I commercianti possono ottenere un checkout semplificato senza memorizzare le credenziali dell'utente, in quanto lo fa l'API, rendendo i commercianti meno vulnerabili agli attacchi;
- La PaymentRequest API dovrebbe facilitare l'introduzione di metodi di pagamento più sicuri sul Web, come i pagamenti con carta tokenizzata;
- I proprietari dei metodi di pagamento disporranno di meccanismi standard per autorizzare software specifici a implementare il loro metodo di pagamento, che il browser può verificare attraverso una firma digitale.

I browser utilizzano una varietà di meccanismi per archiviare informazioni sensibili dell'utente, e attualmente W3C sta sviluppando nuove tecnologie per aumentarne la sicurezza. Per quanto riguarda la memorizzazione delle informazioni delle app di pagamento in modo sicuro, questo è un dettaglio di implementazione che è diverso per ogni app di pagamento, e tale sicurezza è a carico del provider dell'app di pagamento.

3.1 Esempio di un possibile attacco

3.1.1 Descrizione dell'attacco

La sicurezza di usare la PaymentRequest API è che utilizza la gestione delle credenziali del browser che stiamo usando: se stiamo usando Chrome userà la gestione delle credenziali di Google, mentre se stiamo usando Edge userà Microsoft Pay (Nota: in questo caso è necessario anche autenticarsi con l'account Microsoft). Sicuramente il livello di sicurezza è elevato ma non è immune ad un attacco XSS, che potrebbe attaccare similmente al Phishing. L'API apre una finestra dove inserire le credenziali, sicura perchè non vengono scritte nel DOM. Con un attacco XSS, alla chiamata dell'API, invece di questa finestra potrebbe venirne aperta un'altra uguale a quella originale, gestita però dall'attaccante. Essendo identica la vittima sarà convinta di inserire le credenziali in un posto sicuro, mentre invece saranno inviate all'attaccante invece di essere salvate nel browser tramite l'API. Sarà possibile essere vittima di questo attacco solamente la prima volta che saranno inserite le credenziali in quanto l'API chiede l'inserimento delle credenziali solamente la prima volta, dopo saranno salvate e non verrà più chiesto l'inserimento da parte dell'utente. Sia su Chrome che su Microsoft l'inserimento del codice CVV viene chiesto in una pagina successiva, dopo aver inserito tutte le credenziali e averle salvate nella pagina corrente. Un attaccante, per essere sicuro di ottenere anche quel codice potrebbe inserire il form nella prima pagina cosicché l'utente ignaro, inviando le informazioni, manda tutte quelle utili all'attaccante.

3.1.2 Come difendersi

Vi sono diverse metodologie per difendersi da questi tipi di attacchi:

- Una strategia per combattere il phishing è sicuramente quella di istruire le persone a riconoscere gli attacchi e ad affrontarli;
- Dato che il più delle volte non è facile riconoscere questi attacchi, ci sono anche delle misure anti-phishing implementate nei browsers, come estensioni o toolbar, oltre a diversi software contro il phishing;
- Inoltre, la maggior parte dei siti bersaglio del phishing sono protetti da SSL con una forte crittografia, dove l'URL del sito web è usata come identificativo. Questo dovrebbe in teoria confermare l'autenticità del sito, ma nella pratica è facile da aggirare, sfruttando la vulnerabilità che sta nella user interface (UI) del browser. Nell'url del browser viene poi indicata la connessione utilizzata con diversi colori (blocco verde per certificato EV, scritta https in verde, ecc.).

4 Implementazione PaymentRequest API su una pagina d'esempio

4.1 Costruttore

L'oggetto PaymentRequest è costruito passando i seguenti parametri:

- **methodData:** una serie di identificativi del metodo di pagamento e tutti i dati pertinenti. Un identificativo del metodo di pagamento è una stringa che identifica un metodo di pagamento supportato;
- **details:** contiene le informazioni sulla transazione, come gli elementi pubblicitari in un ordine;
- **options:** contiene informazioni aggiuntive che il Wallet potrebbe dover raccogliere.

Nel seguente esempio stiamo consentendo agli utenti di pagare con qualsiasi carta di debito o di credito appartenente alle reti Visa, MasterCard o Amex. L'oggetto details contiene l'importo totale parziale, l'imposta sulle vendite e il totale dovuto; questi dettagli verranno mostrati all'utente nel portafoglio. Bisogna tenere presente che l'API non aggiunge elementi o calcola l'imposta sulle vendite, spetta al commerciante fornire le informazioni corrette. In questo esempio, stiamo vendendo un bene fisico, quindi chiediamo l'indirizzo di spedizione del cliente.

```
1  var methodData = [  
2    {  
3      supportedMethods: ['basic-card'],  
4      data: {  
5        supportedNetworks: ['visa', 'mastercard', 'amex'],  
6        supportedTypes: ['credit']  
7      }  
8    }  
9  ];  
10 var details = {  
11   displayItems: [  
12     {  
13       label: "Sub-total",  
14       amount: { currency: "USD", value : "100.00" } // US$100.00  
15     },  
16     {  
17       label: "Sales Tax",  
18       amount: { currency: "USD", value : "9.00" } // US$9.00  
19     }  
20   ],  
21   total: {  
22     label: "Total due",  
23     amount: { currency: "USD", value : "109.00" } // US$109.00  
24   }  
25 };  
26 var options = {  
27   requestShipping: true  
28 };  
29 var payment = new PaymentRequest(methodData, details, options);  
30
```

4.2 Visualizzazione dell'interfaccia utente, elaborazione del pagamento e visualizzazione dei risultati


Una volta creato l'oggetto PaymentRequest è possibile attivare il browser per visualizzare il wallet con request.show().

Microsoft Wallet


✕

Confirm and pay

www.webstoreurl.com



Pay with

 John Smith •• 5567

▼

Ship to

John Smith

13311 NE 100th St, #100

Seattle, WA 98100

▼

Shipping options

Standard - FREE 5-6 Business days

▼

Email receipt to

johnsmith@outlook.com

▼

Total (USD)

[Show details](#) ▼

\$345.00

Pay

Figura 2: Wallet dopo la chiamata request.show()

I clienti possono selezionare le informazioni di pagamento, l'indirizzo di spedizione e altri campi appropriati e cliccare su Paga quando è pronto. A questo punto, gli utenti dovranno verificare la loro identità: in caso di esito positivo verrà soddisfatta la promise request.show() e verranno restituite al sito Web tutte le informazioni che il cliente ha fornito. Per il metodo di pagamento con carta di base l'oggetto risultante conterrà il nome del titolare della carta, il numero della carta, il mese di scadenza e altri campi pertinenti. Il commerciante può quindi utilizzare queste informazioni per elaborare la transazione sul back-end. Dopo che la risposta è tornata dal server, è possibile utilizzare result.complete('success') per visualizzare la schermata di successo o result.complete('fail') per indicare una transazione fallita.

```

1  // Mostra l'interfaccia utente nativa
2  payment.show()
3  // Quando la promessa e soddisfatta, passa i risultati al tuo server per l'elaborazione
4  .then(result => {
5      return process(result).then(response => {
6          if (response.status === 200) {
7              // Mostra che la transazione ha avuto successo nell'interfaccia utente
8              return result.complete('success');
9          } else {
10             // Mostra nell'interfaccia utente nativa che la transazione ha avuto esito
                negativo
11             return result.complete('fail');
12         }
13     }).catch((err) => {
14         console.error('User rejected request', err.message)
15     });
16 }
17

```



Thank you!



Lorem ipsum dolor sit amet consectetur
adipiscing elit, sed do eiusmod tempor
incididunt lorem ipsum dolor.
Lorem ipsum dolor sit amet.

Continue shopping

Figura 3: Wallet in caso di successo

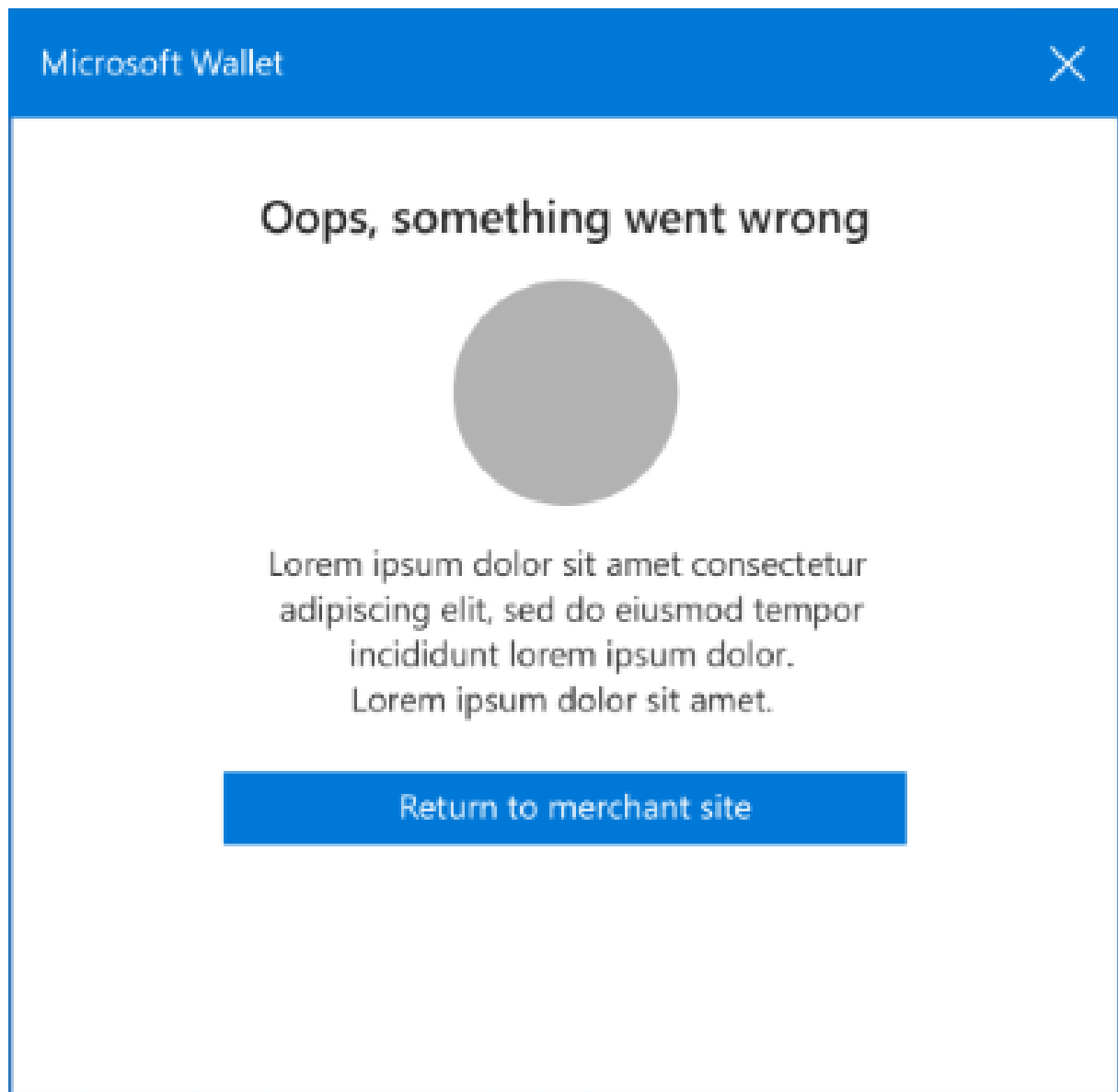


Figura 4: Wallet in caso di fail

4.3 Ascoltare gli eventi

Il prezzo potrebbe cambiare in base all'indirizzo di spedizione e alle opzioni di spedizione selezionate dal cliente. È possibile ascoltare tali modifiche con gli eventi `shippingaddresschange` e `shippingoptionchange` per ricalcolare di conseguenza i prezzi.

```
1 payment.addListener("shippingaddresschange", function (changeEvent) {
2     // Elabora la modifica dell'indirizzo di spedizione
3 });
4
5 payment.addListener("shippingoptionchange", function (changeEvent) {
6     // Modifica delle opzioni di spedizione del processo (ad esempio "spedizione in
7     giornata")
8 });
```

5 Compatibilità web

Desktop						
Mobile						
Feature	Chrome	Edge	Firefox (Gecko)	Internet Explorer	Opera	Safari (WebKit)
Basic support	61	(Yes)	No support ^[1]	?	No support	?

Figura 5: Compatibilità desktop

Desktop							
Mobile							
Feature	Android Webview	Chrome for Android	Edge	Firefox Mobile (Gecko)	IE Mobile	Opera Mobile	Safari Mobile
Basic support	No support	51	(Yes)	No support ^[1]	?	No support	?

Figura 6: Compatibilità mobile

6 Conclusioni

La PaymentRequest API è uno potente strumento per migliorare l'esperienza utente sul Web offrendo ai clienti un'esperienza di acquisto più piacevole, pur avendo delle vulnerabilità difficili da rompere ma dalle quali ci si può difendere.