**Domande generali**

**Qual è lo scopo dell'API di richiesta di pagamento?**

Fare acquisti sul web, in particolare sui dispositivi mobili, può essere un'esperienza frustrante. Ogni sito Web ha il proprio flusso e la maggior parte richiede agli utenti di digitare manualmente gli stessi indirizzi, le informazioni di contatto e le credenziali di pagamento ancora e ancora. Ciò può portare all'abbandono del carrello della spesa e alla perdita della fedeltà dei clienti. Allo stesso modo, è difficile e richiede molto tempo agli sviluppatori di creare e gestire pagine di checkout che supportano vari metodi di pagamento.

L' [API di richiesta di pagamento](https://www.w3.org/TR/payment-request/) (e le specifiche di supporto) consentono ai commercianti di creare esperienze di pagamento semplificate. Piuttosto che ridigitare gli indirizzi di spedizione, le informazioni di contatto, le credenziali di pagamento e altre informazioni ancora e ancora sul Web, gli utenti possono memorizzare e riutilizzare le informazioni e completare più rapidamente e accuratamente le transazioni online.

**In una frase, come funziona?**

L'API di richiesta di pagamento consente a un utente di completare una transazione più facilmente riutilizzando le informazioni memorizzate nel browser o in app di pagamento di terze parti.

**In poche frasi, come funziona?**

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. Il commerciante può inoltre richiedere al browser di creare un'interfaccia utente semplificata per raccogliere l'indirizzo di spedizione, le informazioni di contatto e un numero limitato di elementi aggiuntivi dall'utente.

Il browser determina quale delle "app di pagamento" dell'utente sa di supportare i metodi di pagamento accettati dai commercianti. Il browser mostra le app di pagamento corrispondenti all'utente. Se il commerciante ha chiesto al browser di aiutare a raccogliere un indirizzo di spedizione o altri dati, il browser presenta i dati memorizzati per la selezione dell'utente (o richiede all'utente di inserire nuovi dati).

L'utente seleziona un'app di pagamento da pagare. L'app di pagamento 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.

**Quali sono i principali vantaggi dell'API?**

* Esperienza utente migliorata in vari modi, tra cui: meno tipizzazione, coerenza tra i siti Web, coerenza tra browser e sistemi operativi e nuove funzionalità del browser per semplificare il checkout.
* Conversione aumentata (ovvero: abbandono del carrello inferiore). Anche se non disponiamo ancora di dati significativi per confermare questa aspettativa, Google ha segnalato che il completamento automatico da solo può aumentare le conversioni di 25; questa API intende migliorare sulla funzione di completamento automatico.
* Sviluppo più facile delle pagine di pagamento per i commercianti o i loro fornitori di servizi.
* Miglioramento della sicurezza. L'API di richiesta di pagamento ha il potenziale per ridurre le opportunità di frode e può facilitare l'adozione di metodi di pagamento più sicuri.
* 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.
* Supporta l'innovazione del metodo di pagamento. Riducendo il costo dell'integrazione di nuovi metodi di pagamento, l'industria dei pagamenti può creare e adottare più facilmente nuovi metodi di pagamento, ad esempio per migliorare la sicurezza.

**Quali sono i rischi principali dell'API?**

L'API di richiesta di pagamento consente ai commercianti di "consegnare" la raccolta di credenziali di pagamento alle app di pagamento. Ciò riduce l'onere per i commercianti di creare un'esperienza di pagamento e l'esperienza utente migliorata dovrebbe aumentare le conversioni. Ciò implica, tuttavia, che quando lo fanno, i commercianti non controllano alcuni aspetti dell'esperienza utente.

**Che cosa deve fare un commerciante per utilizzare l'API?**

Ad un livello elevato, l'API influisce sul front end (checkout), non sul back-end. Pertanto, il commerciante non dovrebbe dover apportare modifiche all'elaborazione back-end di vari metodi di pagamento.

Chiunque fornisca la pagina di pagamento del venditore sostituirà i moduli Web con le chiamate all'API di richiesta di pagamento.

**Che cosa deve fare un utente per utilizzare l'API?**

Gli utenti beneficiano del riutilizzo delle credenziali (come informazioni di pagamento, indirizzo di spedizione e informazioni di contatto) che hanno accettato di archiviare nel browser o nelle app di pagamento. Ciò implica che gli utenti hanno bisogno di:

* Un browser o altro agente utente che implementa l'API di richiesta di pagamento;
* Per i metodi di pagamento diversi dalla carta base, l'utente avrà bisogno di una o più app di pagamento;
* L'utente quindi memorizzerà le credenziali nel proprio browser o in altre app di pagamento

Quindi, quando si visita un sito Web che sfrutta l'API di richiesta di pagamento, gli utenti avranno l'opportunità di sfruttare il riutilizzo semplificato delle credenziali archiviate.

**Qual è il ruolo del browser in questa API?**

I browser svolgono due ruoli nell'API. Il primo riguarda queste attività:

* Calcola l'intersezione dei metodi di pagamento accettati dal commerciante e registrati dall'utente.
* Visualizza l'interfaccia utente (nativa) che consente all'utente di fornire informazioni di contatto, indirizzi di spedizione e corrispondenti app di pagamento.
* Fungere da canale per i dati da e verso il commerciante e da e verso l'utente (tramite app di pagamento).

È probabile che anche i browser svolgano un secondo ruolo, agendo come app di pagamento per un piccolo numero di metodi di pagamento. Al momento della stesura di questo documento, i produttori di browser prevedono di supportare i pagamenti della Carta base. Ciò significa che gli utenti saranno in grado di restituire rapidamente le informazioni della carta ai commercianti che sono stati precedentemente memorizzati nel browser.

**Che cosa deve fare un fornitore di app di pagamento per utilizzare l'API?**

Ad un livello elevato, un'app di pagamento deve registrarsi con un browser per dichiarare quale metodo di pagamento supporta.

Le app native di pagamento mobile registrano e comunicano con i browser attraverso meccanismi specifici della piattaforma che sono fuori portata per W3C.

Il gruppo di lavoro Web Payments sta lavorando a un meccanismo per consentire ai siti Web di registrarsi per gestire i pagamenti per conto dell'utente; questo è un lavoro in corso.

**Domande generali sul metodo di pagamento**

**Qual è la differenza tra un metodo di pagamento e un'app di pagamento?**

Nell'ecosistema dell'API della richiesta di pagamento, disaccoppiamo i dati necessari per effettuare un pagamento dal software utilizzato per raccogliere tali dati e avviare l'elaborazione dei pagamenti.

Un metodo di pagamento è caratterizzato dai dati che il commerciante fornisce al pagatore e riceve dal pagatore per essere pagato.

* Esempio: per un metodo di pagamento con carta di base, il commerciante non fornisce dati al pagatore e riceve dal numero di carta del pagatore, dalla data di scadenza, ecc.
* Esempio: per un metodo di pagamento con trasferimento di credito, il commerciante fornisce informazioni sull'account commerciante, ecc. E riceve dalle informazioni del pagatore sulla data di elaborazione, i codici di transazione, ecc.

Un'app di pagamento è il software che l'utente utilizza per pagare. Un'app di pagamento può supportare uno o più metodi di pagamento. Le app di pagamento possono essere implementate utilizzando una varietà di tecnologie, incluse quelle di sistemi operativi nativi o tecnologie Web o di un ibrido. I browser possono anche fungere da app di pagamento, memorizzando le credenziali dell'utente come le informazioni sulla carta. L'API di richiesta di pagamento e l'API di pagamento non risolvono il funzionamento interno delle app di pagamento, ma solo il modo in cui comunicano con il browser.

In generale, più app di pagamento possono implementare lo stesso metodo di pagamento. Tuttavia, vi sono casi importanti in cui è disponibile una sola app di pagamento autorizzata a supportare un metodo di pagamento (proprietario).

**Qual è il significato della distinzione Metodo di pagamento / App di pagamento?**

Nei casi in cui più app di pagamento possono servire un determinato metodo di pagamento (ad es. "Carta base"), il commerciante non deve preoccuparsi dell'integrazione **software**. Il commerciante richiede " dati" attraverso l'API di richiesta di pagamento. Il commerciante (o il suo fornitore di servizi di pagamento) deve gestire tali dati sul back-end, ma non è necessaria alcuna integrazione software aggiuntiva. Allo stesso modo, il disaccoppiamento libera l'utente a scegliere la sua app di pagamento preferita.

**È possibile utilizzare qualsiasi metodo di pagamento con l'API?**

In base alla progettazione, sì. L'API di richiesta di pagamento è progettata per funzionare con un gran numero di metodi di pagamento, inclusi i metodi pull (come i pagamenti con carta) e i metodi push (come i bonifici).

**Come vengono identificati i metodi di pagamento?**

Due strade:

* I metodi di pagamento definiti da W3C sono identificati da stringhe corte come "basic-card". Ogni specifica del metodo di pagamento di W3C include la stringa breve per l'identificazione di quel metodo di pagamento.
* I metodi di pagamento definiti da altre parti sono identificati dagli URL. Ciò consente a qualsiasi parte di pubblicare un metodo di pagamento a cui possono fare riferimento i commercianti.

**Quali metodi di pagamento sono disponibili oggi per essere utilizzati con l'API?**

* Il metodo di pagamento principale è "carta base". Questo è supportato dai browser (che fungono da app di pagamento) e da numerose app di pagamento proprietarie.
* Aggiungi ulteriori informazioni sui metodi di pagamento proprietari che conosciamo oggi.

**Cosa è necessario per creare un metodo di pagamento che funzioni con l'API di richiesta di pagamento?**

Per creare un metodo di pagamento che può essere utilizzato con questa API, sono richieste le seguenti informazioni:

* Un identificatore per il metodo di pagamento; vedere la [specifica dell'identificatore del metodo di pagamento](http://www.w3.org/TR/payment-method-id/) .
* Una descrizione dei dati forniti dal commerciante all'app di pagamento ("dati di richiesta") e i dati restituiti dall'app di pagamento al commerciante tramite l'agente utente ("dati di risposta").

**Domande generali sull'app di pagamento**

**Un'app di pagamento è solo un portafoglio digitale?**

Più o meno. Perché la frase "portafoglio digitale" significa cose diverse per persone diverse, abbiamo scelto un termine diverso.

**In che modo gli utenti ricevono le app di pagamento?**

Ci aspettiamo che ci siano molti modi per scoprire e registrare app di pagamento, tra cui visitare siti Web ("app di pagamento basate sul Web") e scaricare app di pagamento da negozi di sistemi operativi mobili.

**Le app di pagamento sono app native per dispositivi mobili o app Web?**

In base alla progettazione, entrambi. Il gruppo di lavoro Web Payments sta lavorando su una specifica per come le applicazioni Web si registrano per gestire le richieste di pagamento. Il gruppo di lavoro Web Payments non discute l'integrazione di app di pagamento native su piattaforme proprietarie; che viene gestito dai proprietari di quelle piattaforme.

**Come fa il browser a sapere quali app di pagamento ha l'utente?**

Il gruppo di lavoro Web Payments sta sviluppando una specifica che definisce il modo in cui questa registrazione avviene per le app di pagamento basate sul Web. L'obiettivo del gruppo di lavoro Web Payments è stabilire un meccanismo di registrazione unico per i programmi utente su qualsiasi sistema.

Per le app di pagamento create con tecnologia nativa (proprietaria), il browser o il sistema operativo sottostante determinano il meccanismo di registrazione e possono variare da sistema a sistema.

**In che modo il browser determina se un'app di pagamento "corrisponde" a una determinata transazione?**

L'API di richiesta di pagamento definisce un algoritmo che considera:

* Se l'app di pagamento supporta uno qualsiasi dei metodi di pagamento accettati dal commerciante. Il commerciante dichiara quali metodi di pagamento supporta attraverso un elenco di identificativi del metodo di pagamento passati attraverso l'API.
* Inoltre, alcuni metodi di pagamento consentono ai commercianti e alle app di pagamento di descrivere più dettagliatamente le condizioni in base alle quali accettano o supportano tali metodi di pagamento. Questa informazione di "capacità" viene anche utilizzata per determinare se un'app di pagamento corrisponde a una determinata transazione.
* I browser possono anche implementare altre specifiche che hanno un impatto sulla corrispondenza, incluso il [Manifestazione del metodo di pagamento](https://w3c.github.io/payment-method-manifest/) .

**Quali app di pagamento dovrebbe supportare un commerciante?**

Non è compito del W3C raccomandare il software ai commercianti. Tuttavia, riteniamo che sia utile riformulare questa domanda come domande multiple:

* Quali metodi di pagamento desidero accettare (ad esempio pagamenti con carta, bonifici, PayPal, Alipay, ecc.)?
  + I commercianti prendono una decisione aziendale su quali metodi di pagamento scelgono di accettare.
* Cosa è necessario per supportare una particolare app di pagamento?
  + Per i metodi di pagamento proprietari, il proprietario del pagamento determina i requisiti di integrazione del software. Per i metodi di pagamento che possono essere implementati da più app di pagamento, non è prevista l'integrazione del software oltre alla gestione dei dati restituiti dall'app di pagamento tramite l'API di richiesta di pagamento.

**Quali app di pagamento funzionano con questa API oggi?**

Poiché le specifiche sono ancora in fase di sviluppo, oggi non ci sono molte app di pagamento che utilizzano l'API. Siamo a conoscenza di quanto segue:

* Un certo numero di browser implementa la "carta base" e quindi agisce come app di pagamento per quel metodo di pagamento.
* Alcuni browser stanno lavorando per supportare app di pagamento native come Alipay, Samsung Pay, PayPal e altri

**Le app di pagamento possono rifiutarsi di gestire i pagamenti da un determinato sito Web?**

Sì. Una volta selezionati dall'utente e avviati, le app di pagamento possono fare molte cose, tra cui la notifica all'utente che l'app di pagamento non accetta richieste di pagamento dal sito.

**Visualizzazione dell'app di pagamento e domande per l'ordine**

**Come vengono visualizzate le app di pagamento corrispondenti all'utente?**

Dipende dal singolo browser. La visualizzazione può variare da browser a browser, da desktop a cellulare e così via.

**In che modo i commercianti sanno quali app di pagamento ha l'utente?**

Al fine di proteggere la privacy degli utenti, i commercianti hanno accesso a informazioni molto limitate sull'ambiente dell'utente. L'API di richiesta di pagamento supporta un meccanismo di query limitato per consentire al commerciante di determinare se l'utente ha "qualcosa" che può essere utilizzato con l'API di richiesta di pagamento, ma che non fornisce informazioni su software specifico. Questa informazione consente ai commercianti di rilevare il supporto per l'API di richiesta di pagamento e quindi di mostrare una pagina di checkout che utilizza l'API, oppure di creare una pagina di fallback se l'utente non è pronto a pagare con qualche app di pagamento.

**I commercianti possono consigliare le app di pagamento all'utente?**

Sì, tramite il loro sito Web, ma non tramite l'API di richiesta di pagamento. Fino a quando l'utente non ha registrato un'app di pagamento, non è idonea a comparire nell'elenco di app di pagamento corrispondenti per una transazione.

**In che modo i browser determinano l'ordine di visualizzazione delle app di pagamento corrispondenti?**

I browser tengono conto di una varietà di informazioni per fornire la migliore esperienza utente. Queste informazioni includeranno, ad esempio:

* Qualsiasi preferenza utente supportata da un determinato browser; i diversi browser forniranno all'utente diverse opzioni.
* Comportamento dell'utente, come le app di pagamento utilizzate di recente.

**Come cambieranno le pagine di checkout come risultato di questa API?**

I commercianti possono semplificare le pagine di pagamento in diversi modi, tra cui:

* Non avranno bisogno di usare la pagina di checkout per raccogliere la spedizione e altri dati comuni; il browser può fornirlo più rapidamente se l'utente lo ha già archiviato.
* Non avranno bisogno di chiedere agli utenti di scegliere un metodo di pagamento. Invece, possono fornire un singolo pulsante che consente al browser di visualizzare app di pagamento rilevanti.

**Che aspetto ha il pulsante che i commercianti utilizzeranno con questa API?**

Non è necessario utilizzare un particolare pulsante; l'API può essere utilizzata una o più volte su una pagina di pagamento con diversi metodi di pagamento e pulsanti diversi.

W3C può fornire un pulsante riconoscibile in modo che sui siti Web, gli utenti possano prevedere l'esperienza utente che avranno quando preme quel pulsante.

**Qual è l'impatto su altri pulsanti che si vedono in genere in una pagina di pagamento?**

I commercianti hanno la flessibilità di utilizzare l'API in diversi modi.

Alcuni commercianti potrebbero voler sostituire un insieme di pulsanti esistenti (per diversi metodi di pagamento) con un singolo pulsante "Acquista". Con l'API, premendo un singolo pulsante "Acquista" il browser visualizza solo le app di pagamento che possono essere utilizzate con l'elenco dei commercianti dei metodi di pagamento accettati.

Altri commercianti potrebbero voler mescolare i pulsanti esistenti con un nuovo pulsante per l'API di richiesta di pagamento.

**In che modo l'API di richiesta di pagamento influisce sul flusso dei metodi di pagamento che già supporta?**

Oggi, il flusso per gli utenti di solito implica qualcosa del genere:

* Scansione di un elenco di metodi di pagamento accettati (non di cui l'utente si preoccupa)
* Scegline uno e continua
* 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, quindi inviarli di nuovo dopo che il pagamento è stato completato.

L'API di richiesta di pagamento consente un flusso migliorato:

* L'utente preme un pulsante di acquisto singolo (non è richiesta alcuna scansione)
* Il browser visualizza le app di pagamento dell'utente che possono essere utilizzate per la transazione. È probabile che i browser supportino le preferenze dell'utente in modo che, ad esempio, un'app di pagamento venga avviata automaticamente su un determinato sito Web. Ciò semplificherà ulteriormente 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, quindi inviarli di nuovo dopo che il pagamento è stato completato. Il gruppo di lavoro Web Payments sta discutendo, tuttavia, come possiamo migliorare l'esperienza dell'utente creando un senso più forte di "essere ancora nel contesto commerciale" quando si utilizza un'app o un sito Web da pagare. Più lavoro deve essere fatto su questo argomento.

**Una pagina di checkout può utilizzare l'API di richiesta di pagamento anche se non è ancora supportata da tutti i browser?**

Sì. Sono disponibili numerosi strumenti per gli sviluppatori per rilevare il supporto del browser per l'API e la disponibilità di almeno un'app di pagamento. Queste informazioni possono essere utilizzate dallo sviluppatore per adattare dinamicamente la pagina di checkout e fornire una pagina di verifica ("tradizionale") per la retrocompatibilità.

**Domande di backend**

**Che cosa deve fare un commerciante per accettare un particolare metodo di pagamento?**

La risposta dipende dal metodo di pagamento.

Ad esempio, se oggi il commerciante raccoglie i dati della carta di credito tramite un modulo Web, il commerciante (o il fornitore di servizi di pagamento) riceverà gli stessi dati tramite l'API di richiesta di pagamento e dovrà comunque gestirlo, tuttavia ciò avviene oggi.

Altri metodi di pagamento possono comportare l'integrazione di software aggiuntivo, accordi legali, verifica di commercianti, ecc. Ad esempio, un'organizzazione che possiede un metodo di pagamento proprietario potrebbe richiedere l'integrazione del software oltre a ciò che fa l'API di richiesta di pagamento.

**In che modo un commerciante gestisce i dati di risposta ai pagamenti ricevuti?**

Ad un livello elevato, il commerciante riceve gli stessi (o molto simili) dati tramite l'API di richiesta di pagamento (una API JavaScript) che riceveranno tramite un modulo Web. I commercianti (oi loro fornitori di servizi di pagamento) dovranno comunque fare ciò che ordinariamente fanno con tali dati.

**I commercianti che conservano la carta su file possono ancora utilizzare l'API?**

Sì, potrebbe essere utile per l'acquisizione iniziale dei dati.

**Domande di sicurezza**

**In che modo l'API di richiesta di pagamento aumenta la sicurezza?**

* I commercianti possono ottenere un checkout semplificato senza memorizzare le credenziali dell'utente (dato che gli utenti memorizzano le proprie credenziali). Ciò rende i commercianti meno vulnerabili agli attacchi.
* La selezione delle app di pagamento da chrome browser nativo dovrebbe eliminare alcuni comportamenti dannosi che potrebbero influire sulle pagine Web.
* L'API di richiesta di pagamento 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 (ovvero, una firma digitale).

**In che modo il browser memorizza le informazioni in modo sicuro?**

I browser utilizzano una varietà di meccanismi per archiviare informazioni sensibili dell'utente, inclusi cookie, IndexedDB, memoria locale e funzionalità del sistema operativo. W3C sta inoltre sviluppando nuove tecnologie correlate come l'autenticazione Web e l'API di gestione delle credenziali.

**In che modo le app di pagamento memorizzano le informazioni in modo sicuro?**

Questo è un dettaglio di implementazione per ogni app di pagamento. Lo storage nel back-end è interamente a carico del provider di pagamenti.

**È richiesto il gesto dell'utente per attivare l'API di richiesta di pagamento?**

Sì. PaymentRequest.show () richiede il gesto dell'utente, il che significa che deve essere attivato PaymentRequest.show (), ad esempio, tramite un gestore di eventi del pulsante.

**L'API include l'autenticazione dell'utente?**

No.

Esistono (almeno) due tipi di autenticazione utente:

* Autenticazione del commerciante dell'utente (ad esempio, l'utente accede al proprio account con il commerciante).
* Autenticazione delle app di pagamento dell'utente (ad esempio, fornendo un codice CVV, tramite nome / password o tramite autenticazione a più fattori).

Entrambi questi esulano dall'ambito delle specifiche dell'API della richiesta di pagamento.

**L'API di richiesta di pagamento è richiamata in un contesto sicuro?**

Sì, come indicato dal WebIDL nelle specifiche.

Si prega di notare che le implementazioni del browser possono variare in esattamente ciò che supportano. Ad esempio, Chrome considera i seguenti contesti protetti: "https: //", "file: //" e URL localhost.

**Per i metodi di pagamento push, come fa il commerciante a sapere che la risposta al pagamento non è stata manomessa?**

Dipenderà dal metodo di pagamento. Immaginiamo diversi scenari:

* Il fornitore di servizi di pagamento e merchant può comunicare informazioni autoritative fuori banda.
* Alcuni metodi di pagamento possono supportare la firma digitale della parte della risposta all'API della richiesta di pagamento.

**Domande sullo scenario di pagamento**

**L'API indirizza direttamente gli abbonamenti / i pagamenti ricorrenti?**

No, questa versione dell'API non indirizza direttamente gli abbonamenti. L'API può essere utilizzata per raccogliere credenziali che, in combinazione con un accordo out-of-band, possono essere utilizzate per gli abbonamenti.

**Per i metodi di pagamento push, come fa il commerciante a sapere quando è stato pagato?**

Dipenderà dal metodo di pagamento. Immaginiamo diversi scenari:

* In alcuni casi (ad esempio, pagamenti in tempo reale), il commerciante può controllare il proprio account.
* Il fornitore di servizi di pagamento e merchant può comunicare lo stato di pagamento autorevole fuori banda.
* Alcuni metodi di pagamento possono supportare le informazioni sullo stato della firma digitale nella risposta all'API della richiesta di pagamento.

**Domande sulla distribuzione e sullo stato**

**Quali browser implementano questo oggi?**

A partire da settembre 2017, tutti i principali fornitori di browser stanno implementando le specifiche. Le specifiche sono ancora bozze, e non c'è ancora interoperabilità tra browser e piattaforme (ad esempio, mobile e desktop).

**Come faccio a sapere se un determinato browser ha implementato l'API di richiesta di pagamento?**

Attraverso il rilevamento di funzionalità JavaScript standard.

**Quanto sono interoperabili le implementazioni oggi?**

Le specifiche sono ancora bozze e le implementazioni stanno ancora cambiando. Tuttavia, vi sono segni incoraggianti di interoperabilità iniziale.

**Quando ti aspetti un'ampia interoperabilità?**

L'interoperabilità continuerà ad aumentare nel 2017, in particolare sui dispositivi mobili. Non abbiamo ancora una profonda comprensione dei piani di attuazione nel 2018.

**Quando W3C si aspetta che lo standard sia completato?**

* A partire da novembre 2017, W3C prevede che l'API di richiesta di pagamento diventi una raccomandazione W3C entro la metà del 2018. Ciò dipenderà in parte dalla portata delle implementazioni interoperabili.

**L'API di richiesta di pagamento è solo per il Web?**

In teoria, no. In pratica, prevediamo che venga implementato principalmente dai browser e da altri software Web.

**Relazione con altri standard e tecnologie**

**Qual è la relazione con requestAutocomplete?**

Il requestAutocomplete()metodo ( *aka* rAC), una parte del [meccanismo di riempimento automatico](https://www.w3.org/TR/2014/WD-html51-20140617/forms.html#attr-fe-autocomplete) definito nelle specifiche HTML, è [stato progettato per indirizzare casi d'uso](http://www.html5rocks.com/en/tutorials/forms/requestautocomplete/) simili alla parte centrale dell'API di richiesta di pagamento. Tuttavia, insieme al fatto che RAC non è stato adottato da implementatori diversi da Chrome, rAC è limitato in vari modi rispetto all'API della richiesta di pagamento:

* rAC è limitato agli scenari delle carte di credito (e quindi funziona solo con i campi modulo)
* rAC non può raccogliere un meccanismo di pagamento a livello di sistema da sistemi più recenti come Apple Pay
* rAC non è stato progettato per l'integrazione con sistemi finanziari o software di terze parti

L'API di richiesta di pagamento si impegna a risolvere questi limiti e offrire funzionalità aggiuntive.

**Come funziona l'API di richiesta di pagamento con 3D Secure v1?**

Il commerciante / trasformatore invia i dettagli della carta per l'elaborazione, indipendentemente dal fatto che siano stati raccolti tramite API di richiesta di pagamento o modulo Web. In entrambi i casi, se la risposta successiva è un reindirizzamento, l'utente verrà reindirizzato.

Se il pagamento viene elaborato all'interno di un'app di pagamento ed è un pagamento con carta che richiede 3D Secure, l'app di pagamento visualizza una finestra che esegue il rendering dell'URL di reindirizzamento (come avviene con le app mobili native).

**In che modo l'API di richiesta di pagamento funziona con 3D Secure v2?**

A partire da gennaio 2018, il gruppo di lavoro Web Payments dispone di una [task force 3DS](https://github.com/w3c/3ds/) per rispondere a queste domande.

**Qual è la relazione con i messaggi ISO 20022?**

L'API di richiesta di pagamento facilita la raccolta e lo scambio di dati ma è agnostica rispetto ai dati stessi. Se i commercianti ricevono dati tramite un modulo Web o tramite l'API di richiesta di pagamento, devono comunque trasformarli nel back-end nei messaggi e nei formati richiesti dai diversi sistemi di pagamento.

Le specifiche del metodo di pagamento del W3C hanno una relazione leggermente più stretta con ISO 20022 (o altri formati di messaggio) perché descrivono i dati che fluiscono attraverso l'"API" della richiesta di pagamento. W3C sta cercando di allineare i nomi dei campi nelle sue specifiche del metodo di pagamento con quelle usate in altri standard comuni. Si noti che, a rigor di termini, non è necessario per l'interoperabilità poiché i dati devono ancora essere formattati in base ai requisiti di ciascun sistema di pagamento. Comunque aiutiamo l'allineamento terminologico renderà più facile farlo.

**Regole e regole Domande**

**Qual è l'impatto delle API sull'archiviazione delle credenziali di pagamento lato commerciante?**

Poiché il metodo di [pagamento tramite carta di base](https://www.w3.org/TR/payment-method-basic-card/) favorisce l'archiviazione delle informazioni sulle carte da parte dell'utente, ciò può ridurre l'attrito che ha motivato l'archiviazione sul lato commerciale, liberando così i commercianti dal rischio e dalla responsabilità associati all'accesso non autorizzato alle informazioni archiviate.

Inoltre, i siti Web che utilizzano l'API di richiesta di pagamento per ogni transazione evitano l'attrito che può verificarsi quando gli utenti aggiornano i loro numeri di carta di credito e / o le date di scadenza. Dal punto di vista dell'utente, questo evita il fastidio di dover aggiornare un gran numero di siti web merchant ogni volta che viene rilasciata una nuova carta.

Inoltre, l'abilitazione del programma utente per determinare le informazioni di autenticazione dell'utente solleva il commerciante dal dovere di garantire un'autenticazione locale e sufficientemente forte. Inoltre, i browser e altre app di pagamento possono utilizzare le risorse locali come i token biometrici e hardware per autenticare gli utenti in modi che possono essere più convenienti, più sicuri e creare meno attriti per molti utenti e siti.