NORME TECNICHE CHE REGOLANO IL CONTO DI PAGAMENTO
E I SERVIZI DI PAGAMENTO
(Versione n. 7 del 22/11/2017)

1. Introduzione

Le presenti norme tecniche identificano le regole che il cliente è chiamato a rispettare nell'utilizzo del conto di pagamento e che sono disponibili sul sito internet dell'istituto di pagamento.
L'operatività del conto di pagamento può essere effettuata mediante le apposite procedure informatiche rese disponibili sul sito internet dell'istituto di pagamento, previa la sottoscrizione, con firma digitale, dei documenti necessari per l'apertura del conto. Pertanto, chi fosse sprovvisto della firma digitale non può richiederne l'apertura.

Per la descrizione dei servizi fruibili mediante l'App Iconto di rimanda alle "Condizioni generali d'uso dell'App Iconto".

2. Dotazione informatica del cliente

Il Cliente, per accedere al conto di pagamento, dovrà autonomamente provvedere a dotarsi di accesso alla rete internet e di idonee apparecchiature informatiche e programmi che devono costantemente rispondere alle specifiche di sicurezza riconosciute. Il cliente sarà altresì tenuto a custodire con ogni cura l'apparecchiatura informatica di cui si avvale per accedere alle aree riservate.

3. Aree riservate

Le procedure informatiche per operare sul conto di pagamento sono rese disponibili al cliente il giorno successivo all'attivazione del conto di pagamento che, ai sensi dell'art. 6 comma 2 delle condizioni generali che regolano il conto di pagamento, si perfeziona dopo un primo versamento di importo almeno pari ad Euro 100 (cento).
Effettuato il versamento di cui sopra, l'istituto mette a disposizione del cliente due aree riservate, all'interno del sito internet dell'istituto di pagamento, che consentono di accedere al conto di pagamento, gestirlo, consultare la posizione e disporre operazioni di pagamento.

3.1 Tempi di disponibilità delle aree riservate

Le aree riservate sono pienamente disponibili nei giorni e orari seguenti:
Lun - Ven: dalle ore 8:00 alle ore 21:00
Sabato: dalle ore 8:00 alle ore 14:00
Al di fuori degli orari e giorni sopra indicati il servizio potrà essere disponibile compatibilmente con le esigenze di manutenzione ed efficientamento.

L'istituto di pagamento si riserva la facoltà di limitare o sospendere l'accesso alle aree riservate e/o la facoltà del cliente di impartire ordini di pagamento per ragioni connesse alla manutenzione dei propri sistemi informatici o all'efficienza ed alla sicurezza del servizio, qualora riscontri tentativi di accesso non autorizzato, ovvero un utilizzo del conto di pagamento o delle aree riservate anomalo o difforme dalle previsioni del contratto quadro o dalle presenti norme tecniche, preavvisando il cliente quando possibile.

L'istituto di pagamento, non appena possibile, dà comunicazione al cliente di eventuali interruzioni non programmate dell'accesso alle aree riservate.

3.2 Mancato o difettoso funzionamento delle aree riservate

Il cliente, in caso di mancato o difettoso funzionamento delle aree riservate, dovrà darne tempestiva comunicazione al numero verde 800.500.333 o all'indirizzo e mail assistenza.idp@infocamere.it.
Si ricorda che sul sito internet dell'Istituto, nella sezione contatti, è indicato l'orario di disponibilità del Contact Center.
L'istituto di pagamento non risponderà delle conseguenze derivanti dal malfunzionamento delle aree riservate, dovute a cause di forza maggiore o comunque a eventi non imputabili all'istituto di pagamento stesso.
In particolare, l'istituto di pagamento non sarà responsabile:

- del malfunzionamento dell'infrastruttura di sicurezza e dell'aree riservate in genere, conseguenti al non corretto funzionamento delle apparecchiature del cliente;
- della eventuale perdita, alterazione o diffusione dei dati trasmessi attraverso le aree riservate, se dovuta a circostanze non imputabili all'istituto di pagamento stesso.

L'istituto di pagamento, non appena possibile, dà comunicazione al cliente dell'eventuale malfunzionamento delle aree riservate.

3.3 Accesso alle aree riservate

Per accedere alle aree riservate l'istituto di pagamento fornisce al cliente apposite credenziali mediante le quali potrà gestire il conto di pagamento, consultare la propria posizione e disporre operazioni di pagamento.

4. Credenziali

4.1 Rilascio delle prime credenziali

L'istituto di pagamento fornisce al Cliente le credenziali mediante le quali il cliente potrà effettuare il primo accesso alle aree riservate come di seguito descritto:
User ID: una volta che il cliente ha firmato digitalmente i contratti e li ha caricati sul sito internet dell'istituto, viene fornita al cliente la User ID.

Password iniziale: ricevuto il primo versamento sul conto di importo pari o superiore ad Euro 100,00 (cento/00), l'istituto di pagamento fornisce al cliente, mediante posta elettronica certificata, una password con la quale il Cliente avrà accesso alle aree riservate.

Il Cliente ha l'obbligo di NON comunicare a terzi le credenziali rilasciate in questa fase dall'istituto di pagamento e di utilizzarle secondo una condotta diligente.

4.2 Rilascio della One Time Password

Durante la procedura di registrazione il Cliente fornisce un numero di cellullare che sarà utilizzato dall'Istituto per inviare via sms le "one time password".

La one time password, in combinata con le credenziali di cui al par. 4.1, permette di accedere alle aree riservate e disporre operazioni di pagamento. La one time password è numerica, di lunghezza di 8 caratteri ed ha una durata pari a 2 minuti.

4.3. Modifica della password iniziale

Effettuato il primo accesso, il cliente è obbligato ad impostare - mediante l'utilizzo della password iniziale e della one time password inviata al numero di cellulare indicato in fase di registrazione - la password abilitativa e la password dispositiva di seguito descritte:

- la password abilitativa è la credenziale, impostata dal cliente, che in combinata con la one time password, permette di accedere alle aree riservate e visualizzare determinate informazioni del conto di pagamento, consultare la propria posizione, etc. La password è alfanumerica, di lunghezza di almeno 8 caratteri con le seguenti caratteristiche:
  - contenere almeno una cifra, una lettera maiuscola e una lettera minuscola;
  - essere diversa dallo username né contenerlo;
  - non può essere uguale alle ultime tre password;
  - ha durata pari a 6 (sei) mesi.
- la password dispositiva è la credenziale, impostata dal Cliente e preferibilmente diversa dalla password abilitativa, mediante la quale è possibile disporre operazioni di pagamento in combinata con la one time password. La credenziale è alfanumerica, di lunghezza di almeno 8 caratteri con le seguenti caratteristiche:
  - contenere almeno una cifra, una lettera maiuscola e una lettera minuscola;
  - essere diversa dallo username né contenerlo;
  - non può essere uguale alle ultime tre password;
  - ha durata pari a 6 (sei) mesi.

Il Cliente ha l'obbligo di NON comunicare a terzi le credenziali impostate e di utilizzarle secondo una condotta diligente.

4.4. Aggiornamento delle password

L'istituto obbliga ogni 6 (sei) mesi il cliente, per motivi di sicurezza, a modificare sia la password abilitativa che la password dispositiva. Su sua iniziativa il cliente si impegna a modificare le password con maggior frequenza qualora sussistano opportune motivazioni.
Per modificare le password, il Cliente seguirà la procedura guidata disponibile nell'area riservata "web banking".

4.5. Credenziali - Doveri dell'Istituto di Pagamento

L'istituto di pagamento ha l'obbligo di:

- assicurare che le credenziali non siano accessibili a soggetti non legittimati ad utilizzarle, fatti salvi gli obblighi posti in capo al Cliente;
- astenersi dall'inviare credenziali non specificamente richieste, a meno che le credenziali, già consegnate al cliente, debbano essere sostituite;
- assicurare che siano sempre disponibili per il cliente gli strumenti previsti per eseguire la comunicazione di smarrimento e/o furto delle credenziali ai sensi dell'art. 5.
- impedire qualsiasi utilizzo delle credenziali successivo alla comunicazione di smarrimento e/o furto delle stesse ai sensi dell'art. 5.

4.6. Credenziali - Doveri del Cliente

Il cliente è pienamente responsabile della custodia e del corretto utilizzo delle credenziali anche da parte dei delegati ed è tenuto, per sé e per i delegati, a:

- mantenere segrete le credenziali stesse e a custodirle con la massima cura e in luoghi tra di loro separati;
- adottare tempestivamente tutte le misure necessarie per impedire a persone non autorizzate l'utilizzo delle credenziali;
- adempiere con scrupolosa diligenza agli altri obblighi previsti dalle presenti norme tecniche.

4.7. Smarrimento, furto, sottrazione, duplicazione, distruzione e uso non autorizzato delle credenziali

In caso di smarrimento, furto, sottrazione, duplicazione, distruzione delle credenziali e qualunque uso non autorizzato di queste ultime, il cliente deve darne comunicazione all'istituto di pagamento, telefonando al numero verde 800 500 333 e fornire i dati personali (nome, cognome, codice fiscale, documento di identità, luogo e data di nascita, giorno ed ora in cui ha smarrito o sono state derubate le credenziali).
L'istituto di pagamento, entro il giorno lavorativo bancario successivo, dalla comunicazione di smarrimento o furto delle credenziali invierà al Cliente una comunicazione che consentirà di reimpostare le password e recuperare la User ID.

In caso di smarrimento, furto, sottrazione, distruzione delle apparecchiature informatiche utilizzate per accedere alle aree riservate e qualunque uso non autorizzato di queste ultime, il cliente dovrà parimenti adempiere agli obblighi specificamente indicati nel paragrafo che precede.

5. Tentativi di accesso, sessione scaduta, validità di autenticazione

Qualora il Cliente, tentando l'accesso alle aree riservate, valorizza erroneamente le credenziali per più di 3 (tre) volte, l'Istituto provvede a bloccare l'accesso alle aree riservate del Cliente per motivi di sicurezza.
Per il recupero delle credenziali di accesso si rimanda al par. 9.1 e 9.2.
L'Istituto ha definito il periodo massimo dopo il quale le sessioni dei servizi di pagamento via internet inattive vengono automaticamente terminate differenziandolo per area riservata e modalità di accesso; in particolare:

- accesso portale iconto – durata sessione: area riservata "Gestione Conto" 30 minuti e area riservata "Web banking" 20 minuti;
- accesso mediante App Iconto area riservata "Web banking" 15 minuti.

6. Recupero delle credenziali

6.1. Recupero della UserID

Nel caso in cui l'accesso alle aree riservate sia stato bloccato, ai sensi dell'art. 8, l'Istituto mette a disposizione del Cliente una procedura informatica per il recupero della UserID. La richiamata procedura, disponibile sul sito internet dell'Istituto, prevede la compilazione di una serie di dati identificativi del Cliente e, previa verifica della correttezza dei dati immessi, si conclude con l'invio della UserID mediante posta elettronica certificata.

6.2. Recupero delle password

Nel caso in cui l'accesso alle aree riservate sia stato bloccato, ai sensi dell'art. 8, il Cliente per recuperare le password deve rivolgersi all'assistenza telefonando al numero verde 800 500 333 e fornire i propri dati personali (nome, cognome, codice fiscale, documento di identità, luogo e data di nascita).

6.3. Modifica del numero telefonico sul quale ricevere la One time password

Nel caso in cui il Cliente avesse necessità di modificare il numero di cellulare sul quale ricevere la "one time password" l'Istituto mette a disposizione una procedura informatica per la modifica del contatto telefonico accessibile dalle aree riservate. La richiamata procedura si conclude con l'aggiornamento del numero telefonico negli archivi dell'IdP e l'invio di un messaggio di posta elettronica certificata che conferma la modifica effettuata.

7. Sicurezza

L'istituto di pagamento si impegna, per quanto di propria competenza, a mettere in atto, con adeguata diligenza, interventi volti a tutelare la sicurezza e la riservatezza dei dati trasmessi e delle comunicazioni effettuate dal/al cliente per via telematica.

7.1 Sicurezza delle transazioni

L'istituto di pagamento di InfoCamere è costantemente impegnato a tutelare i dati dei clienti attraverso l'adozione dei più moderni sistemi di sicurezza. I sistemi garantiscono transazioni affidabili e sicure; le interazioni on line con i clienti avvengono con il protocollo HTTPS; inoltre, l'istituto di pagamento InfoCamere garantisce il corretto trattamento dei dati personali dei clienti.

Per effettuare transazioni affidabili e sicure è necessario rispettare alcune semplici regole:

- conservare con la massima cura il nome utente, la password abilitativa e la password dispositiva;
- non far conoscere ad altri i propri codici di accesso;
- non inserire i propri codici personali in siti internet raggiunti cliccando su un link presente nelle comunicazioni ricevute via mail o in qualsiasi altro sito che non sia dell'Istituto di Pagamento;
- non rispondere ai messaggi sulla cui autenticità si hanno dubbi;
- visitare i siti web digitando l'indirizzo internet nella barra degli indirizzi;
- modificare periodicamente le credenziali di accesso; e
- installare sul proprio computer software ricevuti da fonti affidabili.

L'istituto di pagamento non chiede mai, attraverso messaggi di posta elettronica, lettere o telefonate, di fornire le credenziali pertanto, non è opportuno rispondere a e-mail, lettere o telefonate che abbiano come oggetto la richiesta di dati personali. In presenza di richieste di questo tipo è opportuno informare immediatamente l'Istituto di pagamento chiamando il numero gratuito 800.500.333.

8. Trasmissione e Protezione delle Informazioni

Ogni volta che si compie una ricerca su un sito internet, vengono trasmesse delle informazioni. Quando si compiono operazioni via web banking, le informazioni trasmesse devono assolutamente essere protette.

8.1 Trasmissione delle informazioni

Per essere certi di interagire in piena sicurezza con l'istituto di pagamento, è necessario adottare alcune precauzioni ed abituarsi a compiere certe verifiche.

1. Disporre di un antivirus.
2. Disporre di un antispyware.
3. Disporre di un firewall.
4. Assicurarsi che il sistema operativo, i programmi per la sicurezza e i programmi che si utilizzano per accedere alla rete siano sempre aggiornati.

5. Verificate l'URL del sito nel quale vi trovate.
6. Verificate che l'indirizzo inizi con "https://".
7. Verificate l'ortografia dell'indirizzo, ad esempio “https://iconto.infocamere.it.
8. Verificare che il lucchetto appaia nel browser.
9. Verificate il certificato SSL.
10. Non dimenticare mai di cliccare sugli appositi link ('Esci', 'Logout') per chiudere la sessione protetta.
11. Proteggere eventuali connessioni Wi-Fi per evitare che intrusi usino la vostra connessione o spiino le vostre operazioni in rete.
12. Mantenere aggiornato il programma di navigazione. E' importantissimo avere installata sempre l'ultima versione disponibile, dato che i miglioramenti vertono principalmente sulla sicurezza.
13. Eliminare le informazioni dalla memoria.
14. Eliminare i file temporanei, i cookies impostati dai siti visitati, le password memorizzate, la cronologia di navigazione. Svuotare il cestino.

8.2. Proteggere le informazioni trasmesse

I computer per comunicare tra di loro necessitano di un linguaggio tecnico comune: è il ruolo della rete, che garantisce la connessione di tutte le macchine al suo interno. Per scambiare quindi informazioni che siano comprensibili solo a colui che invia e a colui che riceve, è necessario utilizzare sistemi di codifica che nessuna altra macchina possa decriptare se dovesse intercettarle.

Attenzione alle reti Wi-Fi

Con una rete Wi-Fi la connessione è prolungata fino a 50 metri oltre la rete fissa gestita dal vostro fornitore di accessi, che ne garantisce anche la sicurezza. La maggior parte di materiale Wi-Fi, per comodità di utilizzo, è configurato per essere di facile installazione e di rapido utilizzo: tutte le opzioni di sicurezza sono quindi in genere disattivate.

Questo pone diversi problemi: un malintenzionato potrebbe 'ascoltare' ciò che circola sulla vostra connessione internet (come le password delle e-mail) e un qualsiasi computer nei paraggi con una carta Wi-Fi potrebbe utilizzare il vostro accesso a vostra insaputa, rendendovi magari responsabile del suo operato.

Guida – Come difendersi dalle frodi informatiche

Per operare in internet senza paure è sufficiente fare attenzione ai rischi ai quali ci esponiamo dal momento che il nostro computer è connesso alla rete. Imparare a conoscere questi rischi, i malware[1], è già un modo per difendersi con efficacia. Di seguito si riporta un elenco, esemplificativo e non esaustivo, dei rischi ai quali il Cliente si espone operando tramite internet:

Phishing: è una frode informatica, realizzata con l'invio di e-mail contraffatte, finalizzata all'acquisizione, per scopi illegali, di dati riservati.
Spam: identifica la ricezione di messaggi non autorizzati (generalmente commerciali) nella propria casella di posta. Il phishing utilizza anche questa tecnica.
Trojan: sono virus che si nascondono all'interno di programmi o di file eseguibili all'apparenza innocui, con lo scopo di raccogliere informazioni o aprire una porta nascosta per accedere al computer dall'esterno.
Worm sono programmi malware in grado di auto-replicarsi: è simile ad un virus come finalità, ma non necessita di legarsi ad altri eseguibili per diffondersi.
I virus sono identificati come frammenti di software che una volta eseguiti infettano dei file nel computer in modo da riprodursi, facendo copie di sé stessi.
Gli spyware sono software che raccolgono informazioni sull'attività in internet dell'utente, senza il suo consenso.
La trasmissione di informazioni: spesso l'utente invia informazioni riservate su internet: è importante assicurarsi che tali dati non possano essere registrati da malintenzionati.

[1] Si definisce malware un qualsiasi programma creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito. Il termine deriva dalla contrazione delle parole inglesi malicious e software e ha dunque il significato letterale di "programma malvagio"; in italiano è detto anche codice maligno.