Caratteristiche dei servizi.

Aggiornamento: Febbraio 3, 2015

intercom s.r.l via piantà 8 , 28010 vaprio d'agogna NO **T** +39 0321 996479 **F** +39 0321 996247 info@intercom.it http://intercom.it

1. Servizio di Posta Elettronica

0 Definizioni

Standard. I servizi fanno riferimento agli standard per l'interoperabilità dei protocolli della rete Internet. In particolare la serie di internet standards e RFC emanate da IETF. In alcuni casi, in mancanza di specifiche si fa riferimento alle best common practices, discusse nell'ambito delle organizzazioni tecniche.

Contenuti pericolosi. Malware. Qualsiasi software, o contenuto, creato con il solo scopo di causare danno più o meno grave al computer su cui viene eseguito, all'infrastruttura di rete, o ad altri elementi; alla raccolta illegale di informazioni, o alla diffusione con mezzi illegali di messaggi, anche pubblicitari; ad usufruire illegalmente di risorse di rete o computazionali di proprietà di altri utenti.

Messaggi non richiesti. "Spam". Messaggi, prevalentemente di natura commerciale, inviati ad un grande numero di destinatari che non hanno espresso preventivamente l'assenso a riceverli.

1.1 Servizio di inoltro (relay)

1.1.1 Servizio di Inoltro. Intercom fornisce ai clienti che ottengono connettività attraverso la propria infrastruttura, e ai clienti che hanno sottoscritto il servizio di Posta Elettronica, un servizio di inoltro (relay) per la posta in uscita.

SMTP relay	smtp.intercom.it

1.1.2 Protocolli. Il servizio supporta il protocollo SMTP, con crittografia TLS e SSL opzionali, mediante i meccanismi smtp, smtps (deprecato) e submission.

1.1.3 Autenticazione del cliente. Il cliente è autorizzato all'utilizzo del servizio di inoltro mediante autenticazione SMTP. L'autenticazione SMTP è implementata mediante SASL (rfc 4222) e i seguenti meccanismi di autenticazione. La crittografia end-to-end della sessione è opzionale.

	cleartext	SSL	STARTTLS
SMTP (port 25)	digest-md5, cram-md5, ntlm, rpa, gssapi		plain, login, digest-md5, cram-md5, ntlm, rpa, gssapi
SMTPs (port 465, deprecato)		plain, login, digest-md5, cram-md5, ntlm, rpa, gssapi	
Mail Submission (porta 587)			plain, login, digest-md5, cram-md5, ntlm, rpa, gssapi

1.1.4 Credenziali di accesso. Il cliente è responsabile dell'utilizzo delle proprie credenziali di accesso, ed è tenuto a conservarle con cura. Il cliente è responsabile, anche economicamente, di quanto venga effettuato mediante l'utilizzo del servizio e delle credenziali personali.

1.1.5 Invio senza autenticazione. Eccezionalmente, esclusivamente i clienti che ottengono connettività direttamente da Intercom possono utilizzare il servizio di inoltro senza autenticazione. Questi clienti sono sottoposti a limitazioni differenti (al punto 1.1.6) e a diverse classi di servizio. L'invio senza autenticazione è sconsigliato. Il servizio non è garantito oltre il 31.12.2015.

1.1.6 Limitazioni sul numero dei messaggi. Il servizio di inoltro consente ai client di inviare un certo numero di messaggi per unità di tempo. Questa imitazione ha lo scopo di tutelare l'infrastruttura, e il cliente stesso, da errori, o abusi di terze parti che utilizzassero la connessione del cliente per veicolare posta non desiderata.

Clienti autenticati mediante SMTP Auth	500 msg/giorno
Clienti non autenticati con IP assegnato da intercom	50 msg/giorno
Clienti non autenticati con IP non assegnato da Intercom	-

1.1.7 Deroga alla limitazione dei messaggi. Le limitazioni di cui al punto 1.1.5 possono essere modificate su richiesta scritta del cliente. Il cliente, richiedendo la deroga, si impegna a non utilizzare il servizio per l'invio di posta non desiderata, e a metter in atto tutti i dispositivi tecnici necessari ad assicurarsi che le proprie credenziali non vengano utilizzate per introdurre messaggi di posta indesiderata, o con contenuti tali da produrre danno all'infrastruttura o ad altri utilizzatori della rete. Il cliente è responsabile, anche economicamente, dell'abuso in tal senso delle proprie credenziali di accesso, o della propria connessione di accesso. Qualora si verificassero episodi tali da pregiudicare il buon funzionamento della rete, che causino ritardi o malfunzionamenti all'infrastruttura, altri clienti, o altri utilizzatori della rete e fosse necessario l'intervento di un team di tecnici, il costo dell'intervento verrà addebitato al cliente.

I limiti disponibili in deroga sono i seguenti:

Clienti Autenticati	Clienti non autenticati con IP statico assegnato da Intercom
1024 msg/ora	-
4096 msg/ora	
12000 msg/ora	

1.1.8 Sistemi preventivi di analisi. Intercom effettua delle analisi sul traffico uscente, utilizzando informazioni che riguardano l'indirizzo IP di invio, le credenziali di autenticazione, i domini di destinazione, gli header del messaggio, al fine di scongiurare l'invio di posta non desiderata da parte di account le cui credenziali venissero utilizzate da parti non autorizzate. Qualora venisse rilevato un traffico anomalo, anche restando nei termini delle limitazioni sul numero di messaggi inviati, l'account potrebbe venire temporaneamente sospeso, e il cliente notificato.

1.1.9 Conformità allo standard. Intercom si riserva di rifiutare, direttamente nel corso della sessione SMTP, i messaggi che rilevasse non conformi agli standard vigenti per l'invio di posta elettronica. Tale rifiuto è comunicato prontamente durante la sessione al software mittente.

1.1.10 Analisi dei messaggi. Intercom si riserva la possibilità di effettuare analisi di natura statistica, o euristica, in maniera aggregata, sul contenuto dei messaggi, allo scopo di rendere più efficaci le misure di protezione della rete da contenuti indesiderati o pericolosi (definizione).

1.1.11 Deroga all'analisi dei messaggi. Il cliente può richiedere che i propri messaggi non vengano sottoposti alle misure di cui al punto 1.1.7 e 1.1.8. In tal caso, il cliente si considera l'unico responsabile, anche economicamente, dei contenuti introdotti, anche suo malgrado ed a sua insaputa nella rete, mediante le sue credenziali di accesso. Qualora si verificassero episodi tali da pregiudicare il buon funzionamento della rete, causati da tale abuso, e fosse necessario l'intervento di un team di tecnici, il costo dell'intervento verrebbe addebitato al cliente. Allo stesso modo verrà addebitato al cliente il costo di un team specializzato necessario a valutare, ed eventualmente fermare, l'invio di messaggi indesiderati ('spam') mediante le credenziali del cliente, o dagli indirizzi IP a lui assegnati.

1.1.12 Limiti sulle dimensioni dei messaggi. L'invio di messaggi è sottoposto ai seguenti limiti:

Dimensione massima di un messaggio di posta	50 Megabytes
Dimensione massima degli allegati	30 Megabytes

1.1.13 Impossibilità di consegnare un messaggio di posta elettronica. Il servizio di relay far il possibile per consegnare ai destinatari richiesti il messaggio. Qualora non fosse possibile, il messaggio verrà trattenuto per un periodo di 5 (cinque) giorni, durante i quali in conformità allo standard verranno effettuati nuovi tentativi di consegna. Al termine del periodo, il mittente verrà notificato dell'impossibilità di consegnare il messaggio (bounce), e il messaggio rimosso.

1.1.14 Conservazione dei messaggi. I messaggi vengono conservati da Intercom sui propri sistemi per il solo tempo necessario ad effettuare la consegna di cui al punto 1.1.11.

1.1.15 Conservazione dei log. Le informazioni tecniche relative all'inoltro di ciascun messaggio di posta vengono conservati ed archiviati secondo le leggi vigenti.

1.1.16 Limitazioni. Il servizio di inoltro dipende dalla disponibilità dei sistemi riceventi: il servizio garantisce che il messaggio verrà inoltrato al successivo sistema di inoltro, come indicato dallo standard. Nessuna garanzia può essere fornita che il messaggio verrà effettivamente consegnato al destinatario finale.

1.2 Servizio di ricezione e conservazione della posta destinata ai clienti

1.2.1 Servizio di ricezione della posta elettronica. Intercom riceve e conserva i messaggi destinati ai propri clienti che abbiano sottoscritto il servizio. Opzionalmente i messaggi vengono sottoposti a screening, relativamente a contenuti indesiderati, fastidiosi o pericolosi.

1.2.2 Protocolli. Il servizio di ricezione supporta il protocollo SMTP, con crittografia TLS e SSL opzionali, mediante i meccanismi SMTP. Ai clienti è fornito accesso alla posta in giacenza mediante i protocolli POP3 e IMAPv4 con crittografia SSL opzionale.

1.2.3 Crittografia. Allo scopo di tutelare la sicurezza dei propri clienti, l'accesso ai servizi POP3 e IMAP4 senza crittografia, è riservata ai clienti che accedono al servizio dalla rete intercom. In ogni caso è consigliato utilizzare un meccanismo dotato di crittografia.

1.2.3 Autenticazione del cliente. Il cliente è autorizzato all'utilizzo del servizio di giacenza mediante autenticazione POP/IMAP. Il cliente è responsabile delle proprie credenziali di accesso. L'autenticazione è implementata mediante SASL (rfc 4222) e i seguenti meccanismi di autenticazione. La crittografia end-to-end della sessione è opzionale.

	plaintext	SSL	STARTTLS
POP3 (porta 110)	digest-md5, cram-md5, ntlm, rpa, gssapi		plain, login, digest-md5, cram-md5, ntlm, rpa, gssapi
POP3s (porta 995)		plain, login, digest-md5, cram-md5, ntlm, rpa, gssapi	
IMAPv4 (porta 143)	digest-md5, cram-md5, ntlm, rpa, gssapi		plain, login, digest-md5, cram-md5, ntlm, rpa, gssapi
IMAPv4s (porta 993)		plain, login, digest-md5, cram-md5, ntlm, rpa, gssapi	

1.2.4 Conformità allo standard. Intercom si riserva di rifiutare, direttamente nel corso della sessione SMTP, i messaggi diretti ai propri clienti, che rilevasse non conformi agli standard vigenti per l'invio di posta elettronica. Il rifiuto viene prontamente comunicato sulla sessione al sistema mittente, a quale spetta il compito di effettuare la segnalazione alla persona mittente.

1.2.5 Tempi di transito. La posta elettronica è un servizio non deterministico. Sebbene intercom si impegni a elaborare e consegnare ciascun messaggio in tempi ridotti e ragionevoli, non sono fornite garanzie sui tempi di transito.

1.2.6 Graylisting. Intercom può utilizzare in funzione del carico un meccanismo di graylisting, allo scopo di discriminare i messaggi che costituiscono posta indesiderata. Tale meccanismo potrebbe introdurre ritardi, in taluni casi, nella ricezione della posta.

1.2.7 Blacklist. Intercom può utilizzare in funzione del carico un meccanismo di blacklist, fornito da **spamhaus.org**. Il sistema identifica gli indirizzi che sono stati segnalati come origine di spam o che ospitano malware e rifiuta temporaneamente di dialogare con essi.

1.2.8 Analisi dei messaggi. Qualora il cliente lo richieda, Intercom effettuerà analisi di natura statistica, o euristica, in maniera aggregata, sul contenuto dei messaggi, allo scopo di rendere più efficaci le misure di protezione della rete da contenuti indesiderati o pericolosi (definizione). I messaggi determinati non conformi verranno segnalati mediante opportuni meccanismi (header specializzati). I messaggi identificati come indesiderati vengono spostati in una apposita cartella accessibile dal protocollo IMAP e dalla webmail.

1.2.9 Contenuti pericolosi. Il servizio facoltativo di cui al punto 1.2.8 potrebbe determinare alcuni contenuti univocamente pericolosi per il cliente. In tal caso, e solo in tal caso i messaggi potranno venire soppressi, e il destinatario notificato della avvenuta soppressione.

1.2.10 Limiti sulle dimensioni dei messaggi. L'invio di messaggi è sottoposto ai seguenti limiti:

Dimensione massima di un messaggio di posta	50 Megabytes
Dimensione massima degli allegati	30 Megabytes

1.2.11 Filtri. La posta ricevuta viene sottoposta all'analisi di un sistema antispam. La configurazione standard della casella di posta inoltra i messaggi che sono stati considerati come posta indesiderata nella cartella '**Junk**', o "Posta indesiderata". Tale impostazione è modificabile dall'apposita interfaccia della webmail. La cartella 'Junk' è accessibile dalla webmail stessa e tramite il protocollo IMAP. I clienti che accedono tramite il protocollo POP3, che non consente di gestire caselle separate, vedono la posta indesiderata come parte della posta ricevuta, e possono provvedere autonomamente a spostarle.

Con la configurazione di default viene assicurato che ogni messaggio ricevuto venga consegnato in INBOX oppure nella cartella Junk. Nessun messaggio viene cancellato senza intervento del cliente finché non sopraggiungono le scadenze al punto 1.2.11.

Il cliente che utilizza il protocollo IMAP può definire dei criteri di filtro ulteriori mediante il protocollo SIEVE. Il protocollo SIEVE consente di cancellare o spostare messaggi sulla base di regole definite dall'utente. In tal caso, è responsabilità del cliente accertarsi che tali regole non producano perdite di messaggi. La webmail offre un'interfaccia per definire i propri filtri.

1.2.12 Conservazione dei messaggi. I messaggi consegnati ai propri clienti vengono conservati per un periodo di 24 mesi. Sebbene Intercom si impegni ad assicurare il servizio, anche in differenti località geografiche. Non è possibile garantire la conservazione dei messaggi in ogni condizione, in caso, ad esempio di calamità naturali, guasti di grande rilevanza e altre cause di forza maggiore. Alcune cartelle hanno un tempo di conservazione minore.

Messaggi in 'INBOX'	720 giorni
Trash	7 giorni
Junk	30 giorni
Tutte le altre cartelle	720 giorni

1.2.13 Backup. Intercom, in aggiunta al proprio storage di posta ridondato, conserva una copia dei messaggi in giacenza, in uno storage geograficamente diverso dal principale, effettuata con cadenza almeno giornaliera. Il backup non garantisce il recupero di tutti i messaggi in giacenza.

1.2.14 Messaggi cancellati. Il servizio non garantisce la conservazione o il recupero dei messaggi esplicitamente cancellati, volontariamente o involontariamente, dal cliente.

1.2.15 Credenziali di accesso. Il cliente è responsabile dell'utilizzo delle proprie credenziali di accesso, ed è tenuto a conservarle con cura. Il cliente è responsabile, anche economicamente, di quanto venga effettuato mediante l'utilizzo del servizio e delle credenziali personali. Il cliente è rappresentato dalle proprie credenziali, a tutti gli effetti, per quanto riguarda l'accesso a informazioni conservate dal servizio.

1.3.16 Conservazione dei log. Le informazioni tecniche relative all'inoltro di ciascun messaggio di posta vengono conservati ed archiviati secondo le leggi vigenti.

1.3 Servizio di inbound relay (MX), antivirus, antispam

1.3.1 Servizio di inbound relay. Il servizio riceve e inoltra i messaggi di posta destinati ai sistemi installati presso la sede del cliente, conservandoli in caso di indisponibilità dei sistemi del cliente. Opzionalmente i messaggi possono essere sottoposti a screening verso contenuti indesiderati.

1.3.2 Protocolli. Il servizio di ricezione supporta il protocollo SMTP, con crittografia TLS e SSL opzionali, mediante i meccanismi SMTP. Il servizio inoltra i messaggi ricevuti verso un endpoint configurato dal cliente, mediante il protocollo SMTP con TLS opzionale.

1.3.3 Raggiungibilità e firewall. Il cliente deve provvedere affinché il proprio sistema di posta sia raggiungibile dagli inbound relay di Intercom. Le seguenti reti originano connessioni relative al servizio.

IPv4	195.72.195.32/28
IPv6	2a01:2d8:1:0::/64

1.3.4 Configurazione del DNS. Qualora il cliente gestisca il DNS in maniera autonoma, è richiesta la seguente configurazione:

```
IN MX      100   a.smtp-in.intercom.it.
IN MX      100   b.smtp-in.intercom.it.
```

1.3.5 Conformità allo standard. Intercom si riserva di rifiutare, direttamente nel corso della sessione SMTP, i messaggi diretti ai propri clienti, che rilevasse non conformi agli standard vigenti per l'invio di posta elettronica.

1.3.6 Tempi di transito. La posta elettronica è un servizio non deterministico. Sebbene intercom si impegni a elaborare e consegnare ciascun messaggio in tempi ridotti e ragionevoli, non sono fornite garanzie sui tempi di transito.

1.3.7 Graylisting. Intercom può utilizzare in funzione del carico un meccanismo di graylisting, allo scopo di discriminare i messaggi che costituiscono posta indesiderata. Tale meccanismo potrebbe introdurre ritardi, in taluni casi, nella ricezione della posta.

1.3.8 Blacklist. Intercom può utilizzare in funzione del carico un meccanismo di blacklist, fornito da **spamhaus.org**. Il sistema identifica gli indirizzi che sono stati segnalati come origine di spam o che ospitano malware e rifiuta temporaneamente di dialogare con essi.

1.3.9 Analisi dei messaggi. Qualora il cliente lo richieda, Intercom effettuerà analisi di natura statistica, o euristica, in maniera aggregata, sul contenuto dei messaggi, allo scopo di rendere più efficaci le misure di protezione della rete da contenuti indesiderati o pericolosi (definizione). I messaggi determinati non conformi verranno segnalati mediante opportuni meccanismi (header specializzati). E' facoltà e responsabilità del cliente filtrare o cancellare tali messaggi.

1.3.10 Contenuti pericolosi. Il servizio facoltativo di cui al punto 1.1.8 potrebbe determinare alcuni contenuti univocamente pericolosi per il cliente. In tal caso, e solo in tal caso i messaggi potranno venire soppressi, e il destinatario notificato della avvenuta soppressione.

1.3.11 Limiti sulle dimensioni dei messaggi. L'invio di messaggi è sottoposto ai seguenti limiti:

Dimensione massima di un messaggio di posta	50 Megabytes
Dimensione massima degli allegati	30 Megabytes

1.3.12 Impossibilità di consegnare un messaggio di posta elettronica. Il servizio di inbound relay inoltra i messaggi ai sistemi del cliente quanto prima. Qualora non fosse possibile, per irraggiungibilità del cliente, il messaggio verrà trattenuto per un periodo di 5 (cinque) giorni, durante i quali in conformità allo standard verranno effettuati nuovi tentativi di consegna. Al termine del periodo, il mittente verrà notificato dell'impossibilità di consegnare il messaggio (bounce), e il messaggio rimosso.

1.3.13 Conservazione dei messaggi. I messaggi vengono conservati da Intercom sui propri sistemi per il solo tempo necessario ad effettuare la consegna di cui al punto 1.1.11.

1.3.14 Conservazione dei log. Le informazioni tecniche relative all'inoltro di ciascun messaggio di posta vengono conservati ed archiviati secondo le leggi vigenti.