Classificazione di informazioni & Specifiche di gestione per terze parti

Introduzione

Non tutte le informazioni hanno lo stesso valore o sono sensibili e classificarle ci aiuta a capire come devono essere protette; dimostra il nostro impegno in tale protezione e ci aiuta a gestirle in modo efficiente.

Ci sono quattro livelli di classificazione:

- Per uso pubblico
- Per uso interno
- Riservato
- Strettamente riservato

La tabella sottostante offre una guida sui tipi di informazioni che rientrano in ciascuna di queste quattro categorie.

Per default, le Informazioni BT saranno classificate Riservate salvo altrimenti indicato.

Se non si è sicuri sulla categoria delle informazioni, rivolgersi al Contatto per la sicurezza BT.

Classificazione	Descrizione generale	Esempi
Per uso pubblico – Cat 1	Le informazioni pubbliche sono informazioni disponibili al personale interno ed esterno a BT.	• Campagne pubblicitarie. • Comunicazioni generiche già di dominio pubblico (ad es. dichiarazioni PR, articoli pubblici su BT) • Informazioni commerciali disponibili al pubblico, come tariffe o offerte pubblicate
Per uso interno – Cat 2	Informazioni BT disponibili a personale BT e altre persone che hanno accesso alla rete di informazioni di BT e dove tale accesso comporti un rischio commerciale minimo per BT. Le informazioni interne possono includere informazioni soggette a obblighi di riservatezza (ad es., e-mail di "nessuna interruzione di attività", relazioni o documenti contrattuali), se le informazioni non sono abbastanza sensibili commercialmente da richiedere la maggiore protezione descritta di seguito.	• Newsletter interne come BT News • Articoli FixIt • E-mail generali, non sensibili (ad es. nessuna informazione commerciale o dati personali limitati, come spiegato nella colonna a sinistra all'interno del messaggio e-mail)
Riservato – Cat 3	Le informazioni Riservate sono informazioni che dovrebbero essere limitate a un pubblico specifico e dove la divulgazione non autorizzata delle informazioni potrebbe danneggiare la reputazione di BT o la loro divulgazione potrebbe danneggiare le persone alle quali si rivolgono tali informazioni (ad es. la quasi totalità dei dati personali di dipendenti o di clienti). Il principio "necessità di sapere" deve essere applicato alle informazioni Riservate.	• Dati di log di sistema; • Informazioni su vendite e marketing commercialmente sensibili; • Piani aziendali locali; • La maggior parte dei dati personali; e • Dati di rischio. • Tutti i dati personali (definiti nella Condizione intitolata "**Protezione delle informazioni**") salvo classificati come Strettamente riservati.

	Raccolta di diversi documenti Riservati In presenza di una serie di documenti "Riservati" in una sede, la classificazione potrebbe necessitare un aggiornamento e questo potrebbe risultare nella riclassificazione di singoli documenti come "Strettamente riservati" o richiedere ulteriori misure di sicurezza per garantirne la sede nei casi in cui: • Insieme potrebbero comportare un danno eccezionale per BT se venissero divulgati; oppure • Se utilizzati in combinazione con altri dati potrebbero costituire un facile bersaglio.	
Strettamente riservato – Cat 4	Le informazioni o i dati Strettamente riservati hanno una circolazione limitata o circoscritta a pochi destinatari; il principio "necessità di sapere" viene applicato rigorosamente (occorre sapere chi ha copie di tali informazioni e chi ne ha accesso). La divulgazione non autorizzata potrebbe essere molto dannosa per BT. Occorre considerare attentamente se le informazioni sono Strettamente riservate perché richiedono i controlli di sicurezza più rigorosi.	• Dettagli di conti bancari • Gli estremi di autenticazione devono essere trattati come Strettamente riservati. • Password di computer, da archiviare in modo sicuro come indicato nelle Specifiche di cifratura di BT • Dati di contabilità finanziaria, non divulgati fino alla pubblicazione del resoconto annuale • Piani commerciali strategici, strategia competitiva, nuovi prodotti strategici, e nuove politiche di marketing • Valutazioni molto sensibili su competitori, partner o appaltatori • Informazioni sensibili sulle risorse umane che potrebbero allontanare un numero notevole di dipendenti • Particolari di importanti piani di acquisizioni, alleanze, divestimenti e fusioni • Dettagli di importanti vulnerabilità sulla rete • Codici di sicurezza clienti, codici master di cifratura, calcoli di chiave, dettagli di transazioni, conti o revisioni • Relazioni di revisioni o risultati con dettagli di gravi difetti/vulnerabilità nelle pratiche o nei processi BT

Come gestire i dati?

I dati saranno gestiti secondo il livello di classificazione in modo che siano correttamente protetti, che siano su un computer, in transito su una rete, comunicati per iscritto o verbalmente.

Abbiamo regole per gestire i dati e le informazioni.

- **Comunicazioni verbali e multimediali** ad es. in conversazione, sui social network, messaggiando, via Skype
- **Documenti cartacei** ad es. stampa, affissione, smaltimento
- **Documenti elettronici** ad es. salvare, inviare email, trasferire, cancellare
- **In applicazioni o sistemi** ad es. centri dati

Abbiamo anche linee guida separate sul livello e tipo di cifratura prevista per proteggere i dati (il nostro "Standard di cifratura").

La gestione di dati comunicati verbalmente e con mezzi multimediali

Rif	Cosa vuoi fare?	Classificazione	Requisiti di gestione	Motivo
HSM10	Voglio postare informazioni su social media / siti di network – ad es. conto personale Twitter	Per uso pubblico	Non contribuire a siti o postare online affermazioni che potrebbero ragionevolmente essere attribuite a BT o che sono diffamatorie nei suoi confronti e potrebbero danneggiare il marchio e la reputazione di BT.	Il rilascio non autorizzato di informazioni o commenti personali potrebbero danneggiare il nostro marchio
		Per uso interno	Non consentito	
		Riservato	Non consentito	
		Strettamente riservato	Non consentito	
HSM20	Voglio presentare o parlare di qualcosa mediante chiamata in conferenza o messaggi interni	Per uso interno	È possibile utilizzare Live Meeting, WebEx, Webjoin e Lync/Skype for Business	I dati per uso interno sono visibili a persone invitate al meeting
		Riservato	È possibile utilizzare Live Meeting, WebEx, Webjoin e Lync/Skype for Business	Le informazioni Riservate sono visibili a persone invitate al meeting
		Strettamente riservato	• È possibile utilizzare Lync/Skype for Business hosted da BT • Occorre verificare chi è in conferenza • Occorre chiudere il meeting in conferenza per non consentire l'accesso ad altri	Lync/Skype for business utilizzano cifratura come indicato nello Standard di cifratura di seguito
HSM30	Voglio parlare di qualcosa via chat live esterna, ad es. su un sito di supporto fornitore come Cisco	Pubblico	Le conversazioni saranno limitate a 'informazioni pubbliche' disponibili al pubblico sul nostro sito	Per impedire la divulgazione non autorizzata di informazioni
		Per uso interno	Non consentito	
		Riservato	Non consentito	
		Strettamente riservato	Non consentito	
HSM40	Voglio parlare di qualcosa di persona o per telefono	Per uso interno	Accertarsi che la conversazione non possa essere intercettata da nessuno che non lavori direttamente per o per conto di BT	Per impedire la divulgazione non autorizzata di informazioni
		Riservato	Come 'Per uso interno' e • Verificare l'identità della persona con la quale si sta parlando e confermare che abbia la "necessità di sapere" prima di comunicare qualsiasi	Per proteggere le informazioni riservate e assicurarsi che siano limitate a quanti hanno necessità di sapere

			informazione riservata • Accertarsi che esista un contratto con le terze parti rilevanti prima di iniziare la conversazione, se del caso (NB. Prima di assegnare o subappaltare il contratto per intero o in parte a terzi occorre ottenere prima il consenso scritto di BT) • Accertarsi che la conversazione non possa essere udita per caso • Non lasciare informazioni "Riservate" su segreterie telefoniche	
		Strettamente riservato	Come 'Riservato' e • Ridurre il più possibile le informazioni 'Strettamente riservate'	
HSM50	Voglio inviare un messaggio/contenuto via SMS/MMS a tutte le parti interessate (interne e esterne)	Per uso pubblico	Il contenuto del messaggio deve essere limitato a 'informazioni pubbliche' disponibili sul nostro sito	Per impedire la divulgazione non autorizzata di informazioni
		Per uso interno	Nessun requisito speciale di gestione	
		Riservato	Assicurarsi che il messaggio sia inviato solo a chi ha necessità di sapere e che non venga divulgato quanto segue: • Dati relativi alla carta di pagamento • Dettagli bancari • Dettagli relativi alla password	Questi 3 elementi sono Strettamente riservati
		Strettamente riservato	Non consentito	

Gestione dei documenti cartacei

Rif	Cosa vuoi fare?	Classificazione	Requisiti di gestione	Motivo
HPD10	Voglio lavorare su contenuti su copia cartacea in strutture di terzi o a casa	Per uso interno	Occorre applicare la politica "libera la scrivania" quando ci si allontana dalla propria scrivania	Per impedire la divulgazione accidentale
		Riservato	Come 'Per uso interno' e • Quando non si lavora ai documenti, toglierli dalla vista e metterli sotto chiave.	
		Strettamente riservato	Come "Riservato"	
HPD20	Voglio stampare	Per uso interno	• Verificare di inviare alla stampante corretta • Non lasciare i documenti nel vassoio di stampa	Per impedire la divulgazione accidentale
		Riservato	Come 'Per uso interno' e	

			• Utilizzare una stampante ad accesso controllato, una stampante connessa ad un PC o una stampante in una stanza ad accesso controllato	
		Strettamente riservato	Come "Riservato"	
HPD30	Voglio utilizzare una stampante che non si trova né in un edificio di Fornitori né a casa mia (ad es. in locali di terzi, in un hotel, ecc.)	Per uso interno	Normalmente questo non è concesso, perché le stampanti sono dotate di memoria e i dati possono essere recuperati. Usa il tuo buon senso... Vuoi davvero che queste informazioni siano visibili ad altri?	I dati e le informazioni sono recuperabili dalla memoria della stampante
		Riservato	Non consentito	
		Strettamente riservato	Non consentito	
HPD40	Voglio portare informazioni cartacee fuori dal mio luogo di lavoro	Per uso interno	Trasportare in una cartella o in una borsa non trasparente	Per proteggere da divulgazione accidentale
		Riservato	Come 'Per uso interno' e • Non portare dati del cliente e/o di pagamenti fuori dagli uffici Fornitori	
		Strettamente riservato	Come "Riservato"	
HPD50	Voglio condividere o inviare informazioni cartacee a parti interne	Per uso interno	• Mettere in una busta e utilizzare il servizio postale interno	Proteggere dalla vista accidentale
		Riservato	• Non apporre la dicitura 'Riservato' sulla busta esterna. • Se le informazioni sono coperte da 'privilegio legale' chiedere consiglio al team legale.	Impedisce a contenuti 'Riservati' di essere visti accidentalmente. La spedizione con avviso di ricevuta offre prova spedizione, firma alla consegna e conferma online di consegna dell'articolo
		Strettamente riservato	• Utilizzare 2 buste e inviare mediante spedizione 'tracciabile' • Non apporre la dicitura "Strettamente riservato" all'esterno della busta • Ottenere il permesso a condividere la copia cartacea dal titolare del documento • Condividere preferibilmente a mano alle persone indicate come autorizzate • Abbinare le copie ai destinatari con un nome o numero in watermarking (se disponibile) • In caso di smarrimento, occorre avviare una pratica di incidente di sicurezza	Impedisce la vista casuale di contenuti Strettamente riservati. La spedizione con avviso di ricevuta offre prova spedizione, firma alla consegna e conferma online di consegna dell'articolo
HPD60	Voglio condividere o	Per uso interno	Accertarsi di avere un contratto con	Vedere HPD50

	inviare copie cartacee a parti esterne	Riservato Strettamente riservato	terze parti come previsto da HSM40. I controlli sono gli stessi della condivisione con parti interne	
HPD70	Voglio inviare un fax	Per uso interno	Occorre accertarsi che la pagina di copertina del fax copra le pagine di contenuto	Per impedire la divulgazione accidentale
		Riservato	• Inviare una pagina di contenuto con una pagina di prova, quindi contattare il destinatario per confermare la ricevuta prima di inviare il contenuto via fax • Se le informazioni sono coperte da 'segreto professionale', consultare il team legale	Per impedire la divulgazione non autorizzata di informazioni
		Strettamente riservato	Non consentito	
HPD80	Voglio smaltire informazioni cartacee	Per uso interno	Occorre utilizzare • un distruggidocumenti • o un cestino dei documenti che non sia facilmente rimovibile	Rifiuti generali e/o cestini per il riciclaggio non sono modalità di smaltimento sicure
		Riservato	Passarlo in un distruggidocumenti impostato su un taglio particelle minimo $\leq$ 160 mm² e normali strisce di particelle di larghezza $\leq$ 2 mm ad es. 2 x 15 mm.	Per proteggere dalla divulgazione informazioni 'Riservate'
		Strettamente riservato	Passarlo in un distruggidocumenti impostato su un taglio particelle minimo $\leq$ 160 mm² e normali strisce di particelle di larghezza $\leq$ 2 mm ad es. 2 x 15 mm utilizzando un taglio incrociato.	Per proteggere dalla divulgazione informazioni 'Strettamente riservate'

Gestione dei documenti elettronici

Rif	Cosa vuoi fare?	Classificazione	Requisiti di gestione	Motivo
HED10	Voglio archiviare informazioni elettroniche sul mio computer portatile/da tavolo	Per uso interno	Utilizzare la cifratura completa del disco prevista dallo Standard di cifratura di seguito.	Questo converte i dati in codici non leggibili non facilmente decifrabili da persone non autorizzate.
		Riservato	Cifratura completa del disco come descritto nello Standard di cifratura di seguito.	
		Strettamente riservato	Cifratura completa del disco come descritto nello Standard di cifratura di seguito.	
HED20	Voglio archiviare i miei documenti su SharePoint o altro sistema di gestione documenti NON ubicato su cloud o con altri Servizi internet	Per uso interno	• Utilizzare livelli e gruppi di permesso per impostare il controllo di accesso secondo il ruolo. Questi devono essere impostati al livello minimo per consentire al personale di svolgere il proprio lavoro • Riesaminare i controlli di accesso ogni anno	Limitare l'accesso e/o le modifiche a quanti hanno necessità di sapere

		Riservato	Come 'Per uso interno' e • Documentare il processo per assegnare il personale ai ruoli • I ruoli e le persone ad essi assegnate devono essere riesaminati ogni 90 giorni • I documenti devono essere criptati come previsto dallo Standard di cifratura di seguito	
		Strettamente riservato	Come 'Per uso interno' e • Documentare il processo per assegnare il personale ai ruoli • I ruoli e le persone ad essi assegnate devono essere riesaminati ogni 90 giorni • I documenti devono essere criptati come indicato nello Standard di cifratura di seguito	
HED30	Voglio archiviare informazioni elettroniche sul cloud o con Servizi online come Google docs, GitHub, btcloud.bt.com, Drobox, Pastebin, Facebook ecc.	Per uso interno	Non consentito.	I servizi online aumentano il rischio di accesso non autorizzato alle informazioni
		Riservato	Non consentito.	
		Strettamente riservato	Non consentito.	
HED40	Voglio archiviare informazioni elettroniche su supporti removibili, ad es. una chiavetta.	Per uso interno	• I dispositivi USB devono essere criptati come previsto dallo Standard di cifratura di seguito Per nessun motivo i dati personali possono essere archiviati su questi dispositivi salvo in forma criptata come previsto dallo Standard di cifratura di seguito.	I supporti removibili possono essere smarriti o sottratti più facilmente di un intero computer, pertanto il rischio di accesso ai dati da parte di persone non autorizzate è più elevato. Per proteggere i dati, occorre convertirli in codici non leggibili che non possono essere decifrati facilmente da persone non autorizzate
		Riservato	Come 'Per uso interno'	
		Strettamente riservato	Come 'Per uso interno'	
HED50	Voglio archiviare documenti elettronici o informazioni BT sul mio computer portatile o dispositivo personale	Per uso interno	Non consentito	Persone non autorizzate potrebbero riuscire ad accedere ai dati BT specialmente se il dispositivo viene smarrito, rubato o smaltito per acquistare un modello nuovo.
		Riservato	Non consentito	
		Strettamente	Non consentito	

		riservato		
HED60	Voglio inviare documenti elettronici o informazioni al mio indirizzo email personale	Per uso interno	Non consentito	Per impedire la divulgazione a persone non autorizzate
		Riservato	Non consentito	
		Strettamente riservato	Non consentito	
HED70	Voglio inoltrare automaticamente a un indirizzo email	Per uso interno	Non consentito	I dati potrebbero essere recuperati da persone non autorizzate se la sicurezza dell'account e-mail, dell'ISP o della connessione internet viene compromessa
		Riservato	Non consentito	
		Strettamente riservato	Non consentito	
HED80	Voglio condividere *internamente* o inviare informazioni elettroniche via email	Per uso interno	Nessun requisito speciale	
		Riservato	• Chiarire che la mail è 'Riservata' • Utilizzare impostazioni sensibili per contrassegnare la mail come 'Riservata' • Idealmente, impostare i permessi su 'Non inoltrare' • Se le informazioni sono coperte da 'segreto professionale', consultare il team legale	Per mantenere il controllo su informazioni riservate
		Strettamente riservato	Come 'Riservato' più • Inviare tramite email Sicura (PEC) • Se l'email sicura non è un'opzione, criptare il file come indicato in Standard di cifratura di seguito prima di inviare • Impostare i permessi su 'Non inoltrare'	Per proteggere le informazioni mentre sono in transito sui network
HED90	Voglio condividere o inviare *all'esterno* informazioni elettroniche via email	Per uso interno	L'invio a parti esterne è consentito solo se si è in possesso di contratto come indicato in HSM40	Per mantenere il controllo su informazioni riservate
		Riservato	Come 'Per uso interno' e • Criptare come previsto dallo Standard di cifratura di seguito • Confermare l'invio all'indirizzo e-mail corretto • Se le informazioni sono coperte da 'segreto professionale', consultare il team legale	
		Strettamente	Come "Riservato"	

		riservato		
HED120	Voglio eseguire il backup di documenti elettronici BT	Per uso interno	• Occorre archiviare i documenti sui drive del network del Fornitore o del sistema di gestione dei documenti Fornitore, come indicato in HED030. • La protezione del documento di cui si è fatto il backup deve essere identica a quella del drive del network, SharePoint. • Se si utilizzano supporti removibili, il dispositivo dovrà essere criptato come indicato nello Standard di cifratura di seguito.	I backup devono avere lo stesso livello di classificazione e protezione dei dati originali
		Riservato	Come 'Per uso interno' e • Criptare il documento come indicato nello Standard di cifratura di seguito prima di eseguire il backup	
		Strettamente riservato	Come "Riservato"	

Gestione dei dati di sistema e applicazione

Rif	Cosa vuoi fare?	Classificazione	Requisiti di gestione	Motivo
HSADE	Voglio archiviare e elaborare informazioni e dati elettronici conservati in un centro dati o su un server di sistema	Per uso interno	Non occorrono requisiti speciali se si osservano tutti i requisiti applicabili di cui sopra per conservare i dati per questa classificazione.	
		Riservato	Occorre seguire i Requisiti per hosting di dati esterni da parte di terzi http://www.selling2bt.com/working/ThirdPartySecurity standards/index.htm	
		Strettamente riservato	Come 'Riservato' più Per proteggere i dati del conto bancario perché particolarmente sensibili applicare i controlli seguenti.	

			Questi hanno precedenza su altri controlli applicabili in questa specifica di sicurezza. 1. Ai conti bancari occorre assegnare un token corrispondente ad ogni persona (conti bancari personali di clienti e dipendenti BT) questo esclude i dettagli del conto bancario aziendale di BT e i dettagli dei vari soggetti giuridici BT). 2. Se un'applicazione conserva solo i conti bancari aziendali, la terza parte può stabilire (secondo i tempi, i costi, le risorse, il numero di conti e il numero di utenti che hanno accesso all'applicazione, ecc.) se BT inizialmente accetterà una soluzione di cifratura. Se una soluzione di cifratura viene accettata, allora BT riesaminerà la decisione quando tutti i conti bancari sono protetti per determinare se è adeguata per il futuro. Questo sarà influenzato dai livelli di rischio e dall'appetito di rischio dell'azienda in generale. 3. Quando si visualizzano i dettagli del conto bancario ad un agente come parte di una procedura aziendale (ad es. per verificare la correttezza dei dati del conto da utilizzare per il pagamento o se si comunica con un cliente, ad es. via e-mail o su una fattura) dobbiamo mostrare solo le ultime 4 cifre del conto bancario (ossia coprire i dettagli del conto bancario). 4. In caso di necessità di accedere al conto bancario per esteso (ad es. per consentire una richiesta di credito o debito da parte di una banca), i dettagli della banca devono essere de-tokenizzati o decriptati e trasmessi alla banca mediante un meccanismo di trasporto criptato che osservi la politica di sicurezza BT. Immediatamente dopo l'uso dei dettagli decriptati o de-tokenizzati, questi dovranno essere eliminati in modo sicuro.	

Standard di cifratura

Controlli generali di crittografia.

Rif	Controllo	Motivo
C1.10	Utilizzare librerie Crittografiche aggiornate	Le librerie Crittografiche vengono aggiornate regolarmente. Oltre ad aggiornare i pacchetti di software come indicato nelle istruzioni dei fornitori, i pacchetti crittografici devono essere riesaminati e aggiornati regolarmente.
C1.20	Per la cifratura, utilizzare solo suite per criptaggio approvate dal settore. Ad es. per TLS SSLv2	Cifre non approvate potrebbero introdurre vulnerabilità
C1.30	Per nuove installazioni, utilizzare l'ultima versione di TLS. Non utilizzare SSL V1,2 & 3	Le versioni precedenti, fino a e inclusa TLS1.0 non sono più considerate sicure
C1.40	Attivare l'algoritmo Perfect Forward Secrecy	Gli algoritmi Perfect forward secrecy impediscono la decifratura di messaggi catturati anche se la authentication private key viene compromessa in futuro

C1.50	Non utilizzare certificati autofirmati	I certificati autofirmati annullano il vantaggio dell'autenticazione del punto finale e diminuiscono sensibilmente la capacità di un individuo di rilevare un attacco man-in-the-middle.
C1.60 **GTS2.370**	Utilizzare una autorità certificante standard nel settore per la gestione dei certificati. Ad es. verisign	Per mantenere un inventario di certificati emessi per vulnerabilità e scadenza di certificati
C1.70	Le password devono essere protette utilizzando una funzione matematica a senso unico non reversibile (ad es. algoritmo Hashing) con un fattore di randomizzazione unico (Salt) per ogni password. NB. SALT sono dati randomizzati utilizzati come un input ulteriore ad una funzione a senso unico che aggiunge un "hash" a una password o passphrase.	I file di password archiviati sono estraibili e come tali tutti i dati immessi devono essere protetti per impedire il recupero di password in testo in chiaro
C1.80	Le password protette come indicato in C1.70 devono essere archiviate lontano dai file di configurazione del sistema e avere controllo di accesso implementato in modo che solo gli utenti autorizzati possano leggerne o copiarne i contenuti.	Non dovrà essere mai possibile recuperare password protette da parte di meccanismi come directory traversal, SNMP walk, configuration dump, o altri che possano consentire tentativi di cracking offline.

Implementazione tecnica di crittografia

Protocolli SSL/TLS	
Utilizzabile	**Non utilizzabile**
TLSv1.3 (tbc - Disponibile in OpenSSL dopo il 5 aprile).	SSLv3.0
TLSv1.2	SSLv2.0
TLSv1.1	
TLS v1.0*	

* TLSv1.0 è già a fine ciclo vitale e può essere sconsigliato in qualsiasi momento a causa di problemi noti. Per motivi di osservanza (ad esempio PCI-DSS) può essere necessario disattivare protocolli come TLSv1.0 e TLSv1.1. Tutti i developer devono essere pronti a disattivare questi protocolli per configurazione.

Dimensioni chiave			
	Simmetrica	**Asimmetrica**	**Curva ellittica**
Brownfield	≥ 112 bits	≥ 2048 bits	≥ 224 bits
Greenfield	≥ 128 bits	≥ 3072 bits	≥ 384 bits

Scambio della chiave	
Utilizzabile	**Non utilizzare**
ECDHE (Effimera (chiave di sessione) Scambio della chiave Diffie-Hellman(chiavi non basate su certificati))	kRSA (Scambio della chiave RSA)
	kDHr (Scambio della chiave Diffie-Hellman con chiave RSA)
	kDHr (Scambio della chiave Diffie-Hellman con chiave DSA)
	kSRP (Scambio chiave Password sicura remota (Secure Remote Password, SRP)) kADH (Scambio chiave anonima Diffie-Hellman)
	kPSK (Scambio della chiave a chiave precondivisa)

La Perfect forward security dovrebbe essere basata su valori Diffie-Hellman Group generati o configurati che comprendono primi "sicuri".

Parametri Diffie Hellman

Parametri Diffie Hellman	
Utilizzabile	**Non utilizzare**
3072-bit Diffie-Hellman Group (migliore – deve essere generato localmente).	I valori di default del server (generare i propri localmente)
2048-bit Diffie-Hellman Group (quasi a fine ciclo vitale – deve essere generato localmente).	

Autenticazione	
Utilizzabile	**Non utilizzare**
aRSA (Autenticazione RSA)	aNULL (nessuna autenticazione)
aECDSA (Autenticazione Elliptic Curve Digital Signature Algorithm)	aDSS (Autenticazione DSS)
	aECDH (Curva ellittica Diffie-Hellman)
	aDH (Diffie-Hellman)
	aDSA (Digital Signature Algorithm)
	aPSK (Chiave precondivisa)
	aSRP (Secure Remote Password)

Cifra/Cifratura	
Utilizzabile	**Non utilizzare**
AES 256 GCM (Rijndael (Standard di crittografia avanzata) - Galois Counter Mode)	eNULL (nessuna cifratura)
AES 128 GCM (Rijndael (Standard di crittografia avanzata) - Galois Counter Mode)	DES (cifratura DES)
CHACHA20/POLY1305 (256)	3DES (cifratura 3DES)
AES 256 CCM (Rijndael (Standard di crittografia avanzata) - (Counter Mode with CBC-Mac)	RC4 (cifratura RC4)
AES 128 CCM (Rijndael (Standard di crittografia avanzata) - (Counter Mode with CBC-Mac)	RC2 (cifratura RC2)
AES 256 CBC (Rijndael Cipher Block Chaining) – quasi a fine ciclo vitale.	IDEA (cifratura IDEA)
AES 128 CBC (Rijndael Cipher Block Chaining) – quasi a fine ciclo vitale.	Seed (Cifratura Seed)
	Camellia (Cifratura Camellia)
	ARIA (Cifratura ARIA)

Algoritmo MAC Digest	
Utilizzabile	**Non utilizzare**
AEAD (Authenticated Encryption Additional Data)	MD5 (Funzione hash MD5)
SHA512 (Famiglia SHA2 - Funzione hash SHA512)	SHA1 (Funzione hash SHA1)
SHA384 (Famiglia SHA2 - Funzione hash SHA384)	SHA (alias per SHA1)
SHA256 (Famiglia SHA2 - Funzione hash SHA256)	