One Time Password per un accesso sicuro alla rete

Portfolio completo di soluzioni OTP per ogni esigenza di utilizzo aziendale

SERVIZI FINANZIARI E RETAIL

AZIENDALI > SOLUZIONI

GOVERNO

TELECOMUNICAZIONI

TRASPORTO

gemalto
security to be free

One Time Password per un accesso sicuro alla rete

Le password statiche sono ormai obsolete

È possibile che il compleanno di suo figlio o il nome del suo animale domestico costi alla sua azienda una quantità significativa di denaro? È possibile che la sua rete aziendale possa essere compromessa da un post-it? Se l'unica barriera che protegge l'accesso alla sua rete è un nome utente e una password, è possibile che questi bit di informazioni personali possano portare ad un accesso non autorizzato e ad un impatto considerevole sulla sua azienda. Una rete compromessa che comporta la perdita di dati aziendali può minare la fiducia nella vostra axienda da parte dei vostri clienti e quindi compromettere il fatturato aziendale. Secondo uno studio del 2009 condotto dal Ponemon Institute, le violazioni dei dati costano alle aziende statunitensi in media 6,75 milioni di dollari l'una. Calcolando i dollari potenzialmente a rischio, risulta chiaro che il tempo delle password statiche è finito.

Indipendentemente dalla politica sulla sicurezza in vigore, nomi utente e password non sono più sufficientemente sicuri. La gente tende a scegliere password facili da ricordare. Se non sono facili da ricordare, allora le scrivono da qualche parte lasciandole dove sono facili da trovare. E anche se i ladri di identità non le trovano o non le indovinano, è possibile indurre socialmente gli utenti a rivelare la loro password. Esistono inoltre sofisticati metodi tecnici per sottrarre le password degli utenti utilizzando malware o spyware. Questo problema risulta ulteriormente accentuato dall'introduzione degli smartphone e dalla sempre crescente mobilità della forza lavoro. É evidente che questa maggiore flessibilità porta con sé il potenziale rischio di violazioni di rete il che pone nuove sfide ai professionisti della sicurezza IT che devono stare un passo avanti ai potenziali violatori allo scopo di proteggere tutti i punti di accesso delle reti.

L'amministrazione delle password è un processo costoso. Per evitare che gli utenti scelgano codici di accesso ovvi e facilmente indovinabili, molte organizzazioni mettono in atto complesse politiche in merito alle password che rendono più difficili gli accessi non autorizzati. Tuttavia l'uso di password complesse causa dei blocchi utente che sono costosi da gestire. Forrester Research calcola che ogni singola chiamata all'help desk da parte di un utente finale costa circa 25 - 50 dollari e che le aziende spendono in media 200 dollari all'anno a persona per la gestione delle password.

- **Protezione di tutti i punti di accesso della propria rete**
- **Soluzioni OTP per ogni esigenza aziendale**
- **Disponibilità immediata all'uso e operatività in pochi minuti**
- **Unica licenza per i token – nessuna licenza ricorrente**
- **Possibilità di cedere il token ad un altro utente**
- **Il server SA fornisce un percorso di migrazione verso l'autenticazione PKI**

Una forte autenticazione è l'unica soluzione

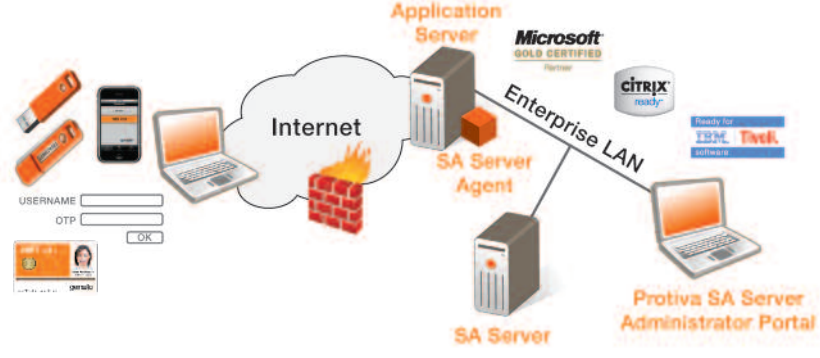
Per risolvere questo problema è necessario introdurre ulteriori livelli di sicurezza che riducano le potenziali minacce dovute a metodi di autenticazione deboli quali l'uso di nomi utente e password. Un'autenticazione forte o multifattore è l'unica risposta possibile a questo problema. Con autenticazione forte si intende un'autenticazione che utilizza diversi fattori per la verifica dell'identità di una persona. I tre fattori maggiormente utilizzati consistono in qualcosa che si conosce, come una password o un PIN; in qualcosa che si ha, come una smart card o un token hardware e in qualcosa che si è, come un'impronta digitale o una impronta della retina.

La soluzione one-time password (OTP) prevede un'autenticazione a due fattori che prevede l'utilizzo di qualcosa che si conosce – come ad esempio un pass code – in combinazione con qualcosa che si ha, in questo caso un token hardware che genera un OTP. Come dice il loro stesso nome, le OTP sono valide esclusivamente per un'unica sessione di connessione o per un'unica transazione dopo di che scadono una volta utilizzate. Consentono di evitare molti inconvenienti associati all'uso delle tradizionali password statiche, il più importante dei quali è che le OTP non sono a rischio di replay attack. In altre parole anche se una OTP viene rubata può essere utilizzata una sola volta. Le soluzioni OTP sono ideali per tutte quelle aziende in cui la forza lavoro remota deve accedere alle proprie risorse quali rete, mail, e pagine web e dove l'accesso a queste risorse deve avvenire tramite Internet o una rete intranet.

Protiva OTP: semplice ma forte

Protiva: il nome del portfolio di soluzioni di autenticazione forte di Gemalto è una piattaforma user-friendly che è stata sviluppata per offrire agli amministratori IT una soluzione flessibile in grado di soddisfare tutte le esigenze di autenticazione. Protiva permette di creare adeguate politiche sui rischi che

Architettura del server SA



garantiscono controlli severi sugli accessi alla rete aziendale e supporta soluzioni che vanno dalle OTP ad una soluzione PKI completa basata sull'uso di smart card. Il fulcro della soluzione Protiva è rappresentato dal server Strong Authentication (SA) Gemalto: una piattaforma di autenticazione flessibile facilmente adattabile alle preesistenti architetture di rete. Il server SA funziona su sistemi operativi Windows e Linux e può essere facilmente integrato in infrastrutture di rete e di autenticazione preesistenti. È disponibile una gamma di soluzioni OTP per ogni esigenza aziendale.

Protiva OTP: forte ma semplice

La soluzione Protiva OTP offre agli utenti finali un'ampia gamma di diversi dispositivi di accesso alla rete portatili, pratici e facili da utilizzare. Proteggono contro key-logging, shoulder surfing, password cracking e contribuiscono a proteggersi dal phishing.

- **Easy OTP** è un token OTP a tempo di facile utilizzo che offre un funzionamento senza connessione. Sufficientemente piccolo da essere agganciato ad un portachiavi, genera una OTP alla semplice pressione di un pulsante per un accesso remoto semplice e sicuro. Le OTP vengono generate con una registrazione oraria che ne consente l'uso in un intervallo temporale limitato..
- La **OTP Display card** è caratterizzata dalla stessa funzionalità della Easy OTP ma è un dispositivo simile ad una carta di credito.

- I **token USB Secure Flash** sono dispositivi di sicurezza personale portatili che supportano sia la funzionalità OTP che quella PKI e garantiscono un sicuro flash storage e applicazioni portatili nonché la firma digitale.
- La **.NET Key** è la soluzione ideale per un uso multiapplicativo di OTP e PKI. Priva di display, garantisce un funzionamento connesso per l'inserimento automatico di OTP.
- **.NET Dual** offre tutti i vantaggi della .NET Key ma genera una OTP tramite un display personalizzabile o un inserimento automatico tramite USB.
- La soluzione **.NET Card** offre un form factor che supporta la OTP per l'accesso remoto quando utilizzata unitamente ad un lettore ma può essere utilizzata anche per implementare servizi PKI. La card .NET può essere utilizzata anche come badge aziendale per l'accesso fisico e logico.

Soluzioni OTP che sfruttano i punti di forza dei telefoni cellulari

Le soluzioni OTP mobili Protiva sfruttano l'ubiquità dei telefoni cellulari per offrire due opzioni di creazione di una OTP sicura senza bisogno di utilizzare un secondo dispositivo fisico.

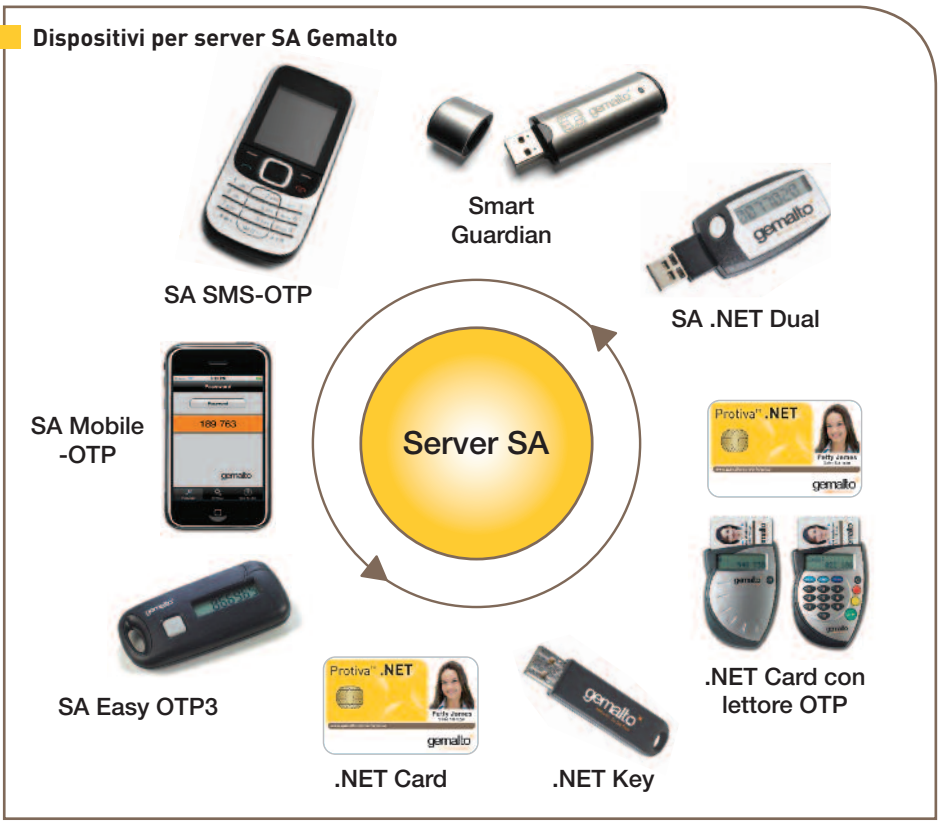
- **SMS OTP** usa il server Strong Authentication per inviare una password a qualsiasi telefono cellulare in formato SMS (Short Message Service). SMS OTP unisce la sicurezza di un'autenticazione a due fattori alla praticità e semplicità dei messaggi SMS. Non è necessario alcun software extra, non ci sono rischi per il telefono del cliente e SMS OTP è facilissimo da utilizzare.
- **Mobile OTP** usa un'applicazione installata su un telefono cellulare che consente agli utenti di generare in tutta sicurezza una OTP utilizzando il proprio telefono cellulare come un token. Non serve alcun hardware aggiuntivo e gli utenti finali possono ottenere la propria OTP tramite un dispositivo che portano sempre con sé, il che rappresenta una soluzione pratica, sicura e di facile utilizzo che ha il vantaggio aggiunto di non aver bisogno di un accesso di rete per poter funzionare. La soluzione supporta un gran numero di apparecchi e per le aziende è facile da implementare e non necessita di alcuna gestione di scorte o di apparecchi sostitutivi.

Tutte le soluzioni OTP di Gemalto sono gestite dal server SA Gemalto. Quando un utente finale inserisce una OTP generata dal proprio dispositivo, l'OTP viene inviata al server SA. Il server verifica la OTP e una volta accertata la sua autenticità autorizza l'accesso. Se un utente finale perde il proprio token o il proprio dispositivo ma risponde in modo corretto ad una serie di domande segrete, allora il server SA creerà un token virtuale e una OTP che potrà essere utilizzata per un unico accesso. È questa flessibilità a rendere unico il server SA: è concepito per semplificare in assoluta sicurezza l'accesso alla rete da parte di utenti autenticati.

Soluzioni flessibili e concepite per evolvere di pari passo alle vostre esigenze aziendali

Le soluzioni Protiva OTP offrono metodi di autenticazione forte semplici e sicuri che possono essere personalizzati a seconda delle varie esigenze aziendali. La tecnologia evolve per soddisfare le esigenze della vostra azienda. Scegliete una soluzione Protiva OTP e, al variare dei rischi e delle esigenze, passate ad un'infrastruttura PKI più completa per un'autenticazione multifattore in grado di offrire funzionalità avanzate quali la crittografia delle e-mail o la firma digitale dei documenti. L'uso di protocolli open ed industry-standard permette l'ottimizzazione dell'hardware e riduce il TCO (costo totale di proprietà). Grazie alla sua flessibilità, sicurezza e semplicità, Protiva è la soluzione più all'avanguardia del settore in grado di ovviare alle limitazioni delle password statiche e di offrire funzioni incorporate a garanzia di soluzioni digitali future più complete.

Dispositivi per server SA Gemalto



> Esempi di applicazioni aziendali

Accesso remoto sicuro a:

- **Informazioni riservate e sensibili**
- **Dati aziendali (Proprietà intellettuale)**
- **CRM – Strumenti di agevolazione delle vendite**
- **Informazioni personali private**

Il leader mondiale nella sicurezza digitale

www.gemalto.com

gemalto
security to be free