

Informazioni su VASCO

VASCO is a leading supplier of strong authentication and e-signature solutions and services specializing in Internet Security applications and transactions. VASCO has positioned itself as global software company for Internet Security serving customers in more than 100 countries, including several international financial institutions. VASCO's prime markets are the financial sector, enterprise security, e-commerce and e-government.



www.vasco.com

SEDE CENTRALE INTERNAZIONALE - Svizzera
Tel. +41 43 555 35 00
e-mail: info-europe@vasco.com

SEDE CENTRALE - Chicago
Tel. +1 630 932 8844
e-mail: info-usa@vasco.com

Sedi di vendita

Area Pacifico e Asia orientale - Singapore
Tel. +65 6323 09 06
e-mail: info-asia@vasco.com

Area Pacifico e Asia orientale - Giappone
Tel. +81 3 5532 7862
e-mail: info-japan@vasco.com

Area Pacifico e Asia orientale - India
Tel. +91 22 4090 7112-14
e-mail: info-india@vasco.com

Australia - Sydney
Tel. +61 2 8061 3700
e-mail: info-australia@vasco.com

Europa, Medio oriente, Africa - Wemmel
Tel. +32.2.609.97.00
e-mail: info-europe@vasco.com

Europa, Medio oriente, Africa - Austria
Tel. +43 1 9043132-0
e-mail: info-europe@vasco.com

America latina - Brasile
Tel. +5511 3443 7541
e-mail: ES-brazil@vasco.com

Stati Uniti - Boston
Tel. +1 508 366 3400
e-mail: info-usa@vasco.com

Stati Uniti - California
Tel. +1 650 378 1202
e-mail: info-usa@vasco.com

Autentichiamo il mondo





AUTENTICHIAMO IL MONDO

VASCO® è uno dei principali fornitori di soluzioni e servizi per autenticazione articolata e firme elettroniche, specializzato nella sicurezza via internet. Ogni giorno, VASCO aiuta i suoi clienti in tutto il mondo a implementare soluzioni di autenticazione forte. I nostri clienti, presenti in oltre 100 paesi del mondo, utilizzano i prodotti VASCO per proteggere diverse applicazioni e transazioni online.

Autenticazione completa per tutte le esigenze

L'approccio a più opzioni di VASCO garantisce l'hosting di tutte le tecnologie di autenticazione sull'esclusiva ed unica piattaforma VACMAN®. La nostra gamma di oltre 50 dispositivi di autenticazione dell'utente finale DIGIPASS®, sia basati su hardware che su software, è completamente integrata nella piattaforma VACMAN.

Le soluzioni VASCO sono molto flessibili: indipendentemente dal settore di attività del cliente, VASCO ha delle soluzioni per tutte le esigenze. Famosa per le sue soluzioni di protezione delle applicazioni bancarie online, VASCO offre lo stesso livello di sicurezza per un'ampia gamma di applicazioni aziendali nei diversi settori verticali, tra cui sanità, gioco online, settore automobilistico, risorse umane, istruzione, amministrazione, e-government, settore legale, catene di distribuzione, produzione e molti altri ancora.

Strategia

VASCO offre una gamma completa di soluzioni e servizi di autenticazione per il settore dei servizi finanziari. Desideriamo aumentare la nostra presenza offrendo queste soluzioni di sicurezza avanzata di tipo bancario ad altri settori, come le aziende commerciali e i settori di vendita alle aziende, vendita ai dipendenti e vendita al dettaglio. VASCO amplia e migliora continuamente la sua linea di prodotti e servizi di sicurezza per soddisfare le esigenze in continua evoluzione dei suoi clienti esistenti e potenziali.

Attività principali

Autenticazione utente

Processo di accesso che controlla che l'utente sia davvero chi dice di essere. La tecnologia DIGIPASS di VASCO sostituisce le insicure password statiche con delle password usa e getta articolate. Queste password sono valide soltanto per un periodo di tempo limitato e non possono essere riutilizzate.

Firma elettronica

Protegge una transazione o un messaggio scambiato tra due parti che si conoscono. Le firme elettroniche offrono una protezione adeguata contro gli attacchi di tipo man-in-the middle e schemi di frodi simili. Consentono di verificare che le informazioni e le transazioni non siano state alterate durante il transito.

Firma digitale

Protegge tramite tecnologia PKI le transazioni e i messaggi tra due parti che non necessariamente si conoscono: è un sistema in cui un ente terzo garantisce l'identità delle parti coinvolte.

La tecnologia PKI consente a banche, aziende ed enti pubblici di firmare transazioni e documenti tramite certificati e chiavi. Le soluzioni PKI garantiscono non ripudio e integrità dei dati.



VANTAGGI DELLA PARTNERSHIP CON VASCO

Capacità di distribuzione e rete di rivenditori estesa

VASCO lavora a stretto contatto con oltre 400 partner e integratori di sistemi in tutto il mondo. Il programma partner VASCO fornisce ai partner:

- Supporto commerciale di marketing tra cui: briefing commerciali, newsletter, assistenza e presentazioni pre-vendita, generazione di lead, dimostrazioni, documenti di marketing specifici per i prodotti, campagne di marketing congiunto, invio di materiale postale, organizzazione di eventi e accesso alla rete extranet per i partner.
- Supporto tecnico e collaborazione con i technical account managers VASCO per la negoziazione dei contratti più importanti
- Formazione e certificazione per consentire ai partner di comprendere adeguatamente tutti gli aspetti della linea di prodotti
- Risorse legate allo sfruttamento di relazioni strategiche: si tratta dei vantaggi dati dalla collaborazione di VASCO con altri fornitori di tecnologia quali Novell, Citrix, Check Point, Cisco ecc.

Solution partner

VASCO ha sviluppato il programma DIGIPASS Ready Partner per rendere possibile la compatibilità tra le soluzioni di altre aziende e la tecnologia DIGIPASS di VASCO. I solution partner possono integrare le loro soluzioni con le soluzioni VASCO oppure sviluppare delle soluzioni nuove basate sull'offerta combinata dei diversi prodotti. I solution partner possono sfruttare una serie di vantaggi pensati per loro, come la presenza nel web, la formazione VASCO, le iniziative di marketing associato, l'assistenza alle vendite, l'assistenza tecnica e la partecipazione agli eventi.

Per i clienti il vantaggio è quello di poter sfruttare dei prodotti integrati in modo più semplice e conveniente e quindi di avere il massimo rendimento sui loro investimenti in fatto di autenticazione. Utilizzando l'infrastruttura di autenticazione e il DIGIPASS già utilizzato per altre applicazioni (accesso remoto, protezione delle applicazioni, crittografia del disco ecc.), il cliente ha un ritorno maggiore sull'investimento.

Per una panoramica completa dei partner VASCO, visitare il sito: www.vasco.com/solutions/partners





BRANDING, DISTRIBUZIONE, STOCCAGGIO... FIDATEVI DI VASCO

Servizi di fornitura

VASCO ha accumulato una vasta esperienza e molte conoscenze sull'implementazione in scala dei progetti di autenticazione. VASCO mette questa esperienza a disposizione dei suoi clienti e consente di diversificare i servizi rispetto alla concorrenza, di focalizzarsi sull'attività aziendale principale e di alleggerire il carico per la catena di distribuzione.

■ Branding e personalizzazione.

I DIGIPASS possono essere personalizzati con i colori e i loghi aziendali così da aumentare il riconoscimento del marchio da parte degli utenti finali.

■ Imballo personalizzato.

VASCO offre un'ampia gamma di servizi di imballaggio: dalla confezione singola o multipla e non personalizzata a imballaggi completamente personalizzati con marchi e loghi.

■ Rinnovamento dispositivi.

Servizio su misura che ha lo scopo di prolungare la vita del DIGIPASS e di ridurre l'impatto economico ed ecologico degli investimenti in fatto di autenticazione.

■ Distribuzione e stoccaggio.

VASCO è in grado di consegnare ovunque nel mondo e offre pertanto anche il servizio di distribuzione a sedi centrali, filiali o utenti finali; è disponibile anche il servizio di stoccaggio dei prodotti del cliente in magazzini protetti e idonei.

Servizi di provisioning

■ Provisioning hardware.

È possibile personalizzare i parametri di sicurezza secondo i requisiti dei reparti di sicurezza aziendali. I dati segreti sono archiviati nell'hardware DIGIPASS tramite un processo approvato e certificato. Per comunicare i PIN iniziali e sbloccare i codici, i reparti di sicurezza aziendali utilizzano metodi con crittografia avanzata.

■ Provisioning software.

Per il provisioning di dati segreti su telefoni mobili o piattaforme di altri fornitori, VASCO offre un servizio di provisioning delle applicazioni che automatizza l'implementazione e la risoluzione di problemi di gestione relativi all'autenticazione basata sul software, consentendo al cliente di focalizzarsi sulla sua attività principale.



Linee di prodotti VASCO

VACMAN®

Piattaforma di autenticazione con nucleo back-end per distribuzioni su grande scala.

Server di autenticazione IDENTIKEY®

Server di autenticazione centralizzato adatto a organizzazioni di tutti i tipi.

IDENTIKEY® Federation Server

Piattaforma di gestione dell'accesso IDENTIKEY. Convalida delle credenziali degli utenti per diverse applicazioni e reti diffuse.

Dispositivo IDENTIKEY®

Dispositivo plug-and-play IDENTIKEY dedicato, per aziende medie e grandi.

aXsGUARD® Gatekeeper

Dispositivi di autenticazione autonomi per l'accesso remoto e la sicurezza Internet.

DIGIPASS® as a Service

Autenticazione basata sul cloud con un modello di servizio gestito.

DIGIPASS®

Dispositivi di autenticazione in grado di fornire un'autenticazione articolata degli utenti e firme elettroniche o digitali. Disponibile in formato software o hardware o come lettore di schede magnetiche.

Soluzioni integrate e OEM

Sicurezza integrata per autenticare le comunità online di tutto il mondo

Settori di destinazione

Sicurezza bancaria online

Sicurezza di conti e transazioni per e-banking e mobile banking.

Sicurezza delle applicazioni online

Accesso protetto ad applicazioni fondamentali per l'azienda (portali, SaaS, e-commerce, giochi online, applicazioni cloud ecc.).

Sicurezza per le grandi aziende

- Accesso remoto protetto per clienti, partner e dipendenti in movimento.
- Sicurezza di rete per le grandi aziende.
- Applicazioni web protette.

E-government

Autenticazione utente per proteggere le applicazioni degli enti pubblici e accelerare la fornitura di servizi online.





CONTRASTARE LE FRODI ONLINE

Online banking protetto

Le banche di tutto il mondo forniscono sempre più strumenti e servizi finanziari online e per dispositivi mobili sia per offrire ai loro clienti un modo più comodo per gestire le proprie transazioni bancarie, sia per migliorare l'efficienza e ridurre i costi di esercizio. Tuttavia l'online banking ha i suoi rischi.

I conti bancari online sono spesso presi di mira dai criminali informatici e le tipologie di frodi diventano sempre più complesse. La sicurezza è sempre la maggiore preoccupazione per i clienti e le aziende. Di conseguenza, le banche devono implementare delle misure di sicurezza adeguate per proteggere la loro infrastruttura e i loro clienti.

Aumentare il livello di fiducia dei clienti

VASCO aiuta le banche e gli istituti finanziari a proteggere i loro canali online. In qualità di azienda leader nel settore della autenticazione forte, VASCO offre un potente sistema di autenticazione a due fattori e soluzioni PKI per soddisfare le esigenze delle organizzazioni finanziarie.

Implementando la nota tecnologia DIGIPASS di VASCO, le banche possono autenticare i loro clienti e ridurre i rischi legati al phishing, all'hacking, ai trojan e agli attacchi man-in-the-middle (MITM). La protezione dei servizi online aumenta notevolmente la fiducia dei clienti e consente alle banche di contare su un vantaggio competitivo duraturo.

Soluzioni su misura

VASCO ha una grande esperienza nell'implementare progetti di autenticazione su larga scala, con milioni di utenti finali; tuttavia è in grado di offrire anche a piccole e medie banche delle soluzioni su misura per le loro specifiche esigenze.

Offriamo un'ampia gamma di soluzioni back-end e dispositivi per gli utenti finali, che vanno da strumenti di autenticazione OTP software e hardware a dispositivi di firma elettronica per la convalida delle transazioni e di firma digitale tramite tecnologia PKI.

Soluzioni di autenticazione VASCO per tutte le esigenze

Back-end

- **Controller VACMAN**
Tecnologia di autenticazione principale di VASCO, adatta a grandi implementazioni
- **Server di autenticazione IDENTIKEY**
Server di autenticazione centralizzato per banche di piccole e medie dimensioni alla ricerca di cicli di implementazione brevi. Il server di autenticazione IDENTIKEY Banking Edition è una soluzione completa per combattere gli attacchi MITM.
- **DIGIPASS as a Service**
Autenticazione basata sul cloud in un'offerta di servizio gestito.

Per gli utenti

- **Famiglia DIGIPASS**
Gamma di oltre 100 dispositivi di autenticazione tra cui dispositivi a un pulsante e tastiere PIN, lettori di schede (EMV CAP) e soluzioni basate su software.
- **DIGIPASS CertiID™**
Soluzione PKI di VASCO basata su client per una autenticazione articolata dell'utente e per la firma delle transazioni.



SFRUTTARE AL MASSIMO L'AUTENTICAZIONE

Servizi di consulenza VASCO

I servizi di consulenza VASCO sono stati pensati come complemento dell'offerta di soluzioni di autenticazione articolata e offrono una gamma di opzioni di servizi di qualità che consentono ai clienti di ottenere il massimo dal loro investimento in strutture di autenticazione.

L'esperienza VASCO è a disposizione di chiunque sia alla ricerca di informazioni sulle sfide attuali in termini di sicurezza e sulle minacce all'e-banking, all'e-commerce e alla sicurezza delle reti, ma anche di chi desidera dei consigli prima o durante l'implementazione.

Tramite la condivisione della sua esperienza, della sua metodologia convalidata e delle sue migliori prassi, VASCO aiuta i clienti a ridurre il tempo di commercializzazione dei loro progetti di autenticazione. VASCO mette a disposizione dei clienti l'esperienza combinata di migliaia di implementazioni di sistemi di autenticazione articolata realizzate con successo in tutto il mondo.

Il nostro team di consulenti è composto da ingegneri e specialisti nell'implementazione, nella fornitura e nell'assistenza ai clienti. I consulenti VASCO sono pronti a fornire tutti i consigli professionali necessari per implementare con successo i sistemi di autenticazione.

Offerta

VASCO offre i seguenti servizi di consulenza:

- **Consulenza prima dell'implementazione**
Focalizzazione sulle minacce, sui meccanismi di difesa della sicurezza dell'e-banking e sulle migliori prassi per l'implementazione di sistemi di autenticazione articolata per le applicazioni e-banking e per dispositivi mobili.
- **Consulenza durante l'implementazione**
Consulenza specifica sul prodotto da implementare.
- **Consulenza dopo l'implementazione**
Focalizzazione sul rilevamento e sull'analisi delle frodi.
- **Consulenza on demand**
Servizi di consulenza specifici per esigenze specifiche.

Per ulteriori informazioni sui nostri servizi di consulenza, visitare il sito: www.vasco.com/consulting

Insieme agli esperti VASCO abbiamo analizzato i diversi modi di utilizzo dei nostri dispositivi DIGIPASS con il controller VACMAN. La loro consulenza non solo ci ha permesso di avere miglioramenti importanti e significativi, ma ci ha permesso anche di innalzare complessivamente il nostro livello di protezione. La collaborazione con VASCO ha apportato valore ed esperienza al nostro progetto: per questo consideriamo VASCO un partner aziendale di valore.

Daniel Ratincx, Responsabile di Delen-Online presso Bank Delen

BANK DELEN
PRIVATE BANKERS



QUANDO IL PROGETTO DI AUTENTICAZIONE DIVENTA UN SUCCESSO

Servizi professionali

I servizi professionali VASCO sono stati pensati per assistere i clienti, i rivenditori, i partner e gli integratori nell'implementazione dei loro progetti di autenticazione articolata. Condividendo la nostra esperienza consentiamo ai nostri clienti di ridurre al minimo le sfide e ottenere i massimi risultati dai progetti di autenticazione, rispettando i limiti di tempo e di budget. I servizi professionali VASCO mettono a disposizione dei clienti i molti anni di esperienza dedicati all'implementazione di progetti di autenticazione a due fattori.

La nostra offerta

Ogni progetto di autenticazione è unico. Diversi clienti hanno diverse esigenze. Qualunque sia il motivo alla base della scelta di una soluzione di autenticazione forte, VASCO ha ingegneri e project manager qualificati per trasformare in un successo il progetto di autenticazione.

Il nostro team dei servizi professionali utilizzerà la metodologia VASCO convalidata:

- Definizione dell'ambito del progetto
- Progettazione della soluzione appropriata
- Implementazione dei prodotti e delle soluzioni
- Creazione delle applicazioni adeguate alle esigenze del cliente
- Assistenza del partner del cliente o del team in-house per l'intera durata del progetto
- Certificazione dell'applicazione del cliente secondo gli standard di settore
- Esame delle implementazioni esistenti e consigli per l'ottimizzazione

Vantaggi

- **Un team di esperti**
I nostri ingegneri esperti e certificati garantiscono un'integrazione senza problemi dell'autenticazione nelle applicazioni o nell'infrastruttura esistenti, utilizzando la metodologia VASCO convalidata.
- **Costo totale di possesso**
Realizzazione di progetti che rispettano i limiti di tempo e di budget
- **Metodologia convalidata**
Implementazione in breve tempo, assistenza per l'intera durata del progetto e sicurezza avanzata per accesso remoto, LAN, applicazioni online e ambienti e-banking e mobile banking.



La Oman Arab Bank fornisce servizi di e-banking protetti con tecnologia DIGIPASS per evitare il furto di identità.

La Oman Arab Bank offre ai suoi clienti privati e aziendali un'ampia gamma di servizi online; è l'unica banca del paese a offrire un servizio di pagamento delle bollette immediato ai fornitori di servizi telefonici. La banca, inoltre, offre dei servizi online agli enti pubblici e si è imposta come fornitore leader di servizi e-banking.

Per proteggere i suoi clienti dalle frodi, la banca ha adottato la nota tecnologia DIGIPASS di VASCO unita al software di autenticazione IDENTIKEY Authentication Server. È stato possibile integrare perfettamente IDENTIKEY Authentication Server nell'infrastruttura della banca; questo ha consentito alla Oman Arab Bank di aggiungere un'autenticazione articolata ai suoi diversi canali e applicazioni. Per la base di clienti privati e aziendali sono stati implementati DIGIPASS GO 6 e DIGIPASS 260, due sistemi che consentono ai clienti l'accesso protetto al loro conto in qualsiasi momento e ovunque si trovino. Grazie all'integrazione della tecnologia DIGIPASS, la banca è stata la prima banca mediorientale a offrire dei servizi ATM senza carta.



بنك عُمان العربي
OMAN ARAB BANK



SEB implementa DIGIPASS 260 e DIGIPASS 920 per garantire l'accesso protetto all'ID della banca e per altre applicazioni online



In qualità di banca leader in Svezia, SEB voleva implementare una soluzione per proteggere i suoi clienti in modo sicuro. La banca voleva implementare una soluzione di facile adozione e indipendente dalla persona. La soluzione doveva offrire un elevato livello di sicurezza e doveva essere in grado di resistere alle minacce alla sicurezza presenti e future. SEB conosceva già la tecnologia di autenticazione VASCO, in quanto aveva già implementato DIGIPASS 260. Tramite l'implementazione di DIGIPASS 920, la banca ha aggiunto un livello di protezione alle sue applicazioni bancarie online e fornisce ora ai suoi clienti una soluzione che rende possibile accedere in modo sicuro all'ID della banca.

SEB

HSBC Bank Brazil fornisce il servizio di mobile banking utilizzando il sistema VASCO DIGIPASS for Mobile

HSBC è la prima banca in Brasile a offrire dei servizi di mobile banking integrato basati sulla tecnologia VASCO DIGIPASS for Mobile. I clienti privati di HSBC possono ritirare contanti dal bancomat utilizzando il telefono come dispositivo di autenticazione. Non basandosi su fornitori esterni, questa tecnologia elimina i problemi di dipendenza dal fornitore e le limitazioni di rete.

DIGIPASS for Mobile consente agli istituti finanziari di lanciare rapidamente i servizi di mobile banking. La soluzione ha consentito a HSBC di aumentare la portata dei suoi servizi finanziari per mezzo di un accesso multicanale. Per la sua collaborazione con HSBC Brazil e l'implementazione di DIGIPASS for Mobile, la nota rivista brasiliana dedicata al mondo bancario "Relatorio Bancario" ha assegnato a VASCO il premio "Best Security Solution".



HSBC



**PROTEZIONE CONTRO IL FURTO DI DATI.
I BENI AZIENDALI SONO AL SICURO.**

**DEDIZIONE. IMPEGNO.
CLIENTI SODDISFATTI.**

Accesso remoto protetto

La protezione delle risorse aziendali e dei dati riservati è essenziale per tutte le organizzazioni. Da quando la forza lavoro è distribuita e sempre più in movimento, l'accesso remoto protetto alle reti e alle informazioni aziendali fondamentali è diventato una necessità per le aziende di tutto il mondo.

L'accesso alle risorse aziendali in qualunque momento e ovunque ci si trovi rappresenta una vera sfida per la sicurezza dei dati, specie da quando la scelta di dispositivi mobili come smartphone, tablet e palmari è diventata una tendenza a crescita esponenziale.

Oltre a ripensare le politiche di sicurezza aziendale e le modifiche infrastrutturali, le aziende devono anche pensare all'utente finale. L'obiettivo è implementare una soluzione di sicurezza adeguata senza compromettere la semplicità d'uso e l'efficienza.

Password dinamiche e firme digitali

VASCO Data Security, leader mondiale nelle soluzioni e nei servizi di autenticazione, fornisce alle aziende di tutte le dimensioni le soluzioni più avanzate per soddisfare le loro esigenze di sicurezza. Grazie alla tecnologia DIGIPASS, VASCO porta nel settore della gestione aziendale un grado di sicurezza di livello bancario grazie alla sua capacità di sostituire le deboli password statiche con password usa e getta, che eliminano una volta per tutte il rischio di accesso non autorizzato a reti, applicazioni e dati.

DIGIPASS consente di accedere in modo sicuro alla rete aziendale, a Windows, ad Outlook Web, a Citrix e a molti altri servizi.

Le transazioni online e i documenti riservati possono essere protetti con una firma elettronica o digitale per garantire che le informazioni non vengano alterate durante il transito.

La sicurezza deve facilitare il lavoro, non ostacolarlo

Per tutte le organizzazioni del mondo è fondamentale che le loro applicazioni aziendali siano attive, continuamente in esecuzione e accessibili in modo sicuro. È necessario però fare in modo che l'autenticazione non sia considerata un fastidio, ma un elemento facilitatore.

VASCO offre un'ampia gamma di pacchetti di assistenza e servizi di supporto tecnico per ambienti di tutte le dimensioni e di tutti i tipi. VASCO è in grado di semplificare la vita con una copertura a risposta rapida in tutto il mondo e piani di servizio flessibili per tutte le esigenze e i budget.

VASCO ha una risposta personalizzata per tutti i tipi di clienti: da accordi di assistenza di base fino ad accordi sul livello del servizio (SLA), per garantire un intervento rapido ovunque nel mondo.

Le diverse opzioni di servizio VASCO consentono di personalizzare l'esperienza di assistenza. I seguenti piani di assistenza tecnica VASCO si adattano a tutte le esigenze.

- Assistenza standard
- Assistenza 24/7
- Assistenza VIP
- Pay-Per-Incident
- Pacchetto di assistenza remota
- Assistenza di emergenza

Offerte di assistenza

VASCO offre un'assistenza specifica per i diversi tipi di utenti.

- I clienti del settore bancario e della sicurezza delle applicazioni possono scegliere diversi pacchetti di assistenza standard che vanno dall'assistenza standard durante l'orario d'ufficio, all'assistenza 24/7, all'assistenza basata su accordo sul livello del servizio (SLA), all'assistenza di tipo pay-per-incident, all'assistenza remota
- Per i clienti nel settore della sicurezza aziendale, l'assistenza tecnica viene fornita dal rivenditore o dall'integratore del sistema. È possibile tuttavia richiedere l'assistenza tecnica diretta da parte degli esperti di VASCO.
- I distributori, gli integratori di sistema e gli ingegneri certificati VASCO possono disporre dell'assistenza tecnica standard durante l'orario d'ufficio.
- Ai rivenditori VASCO, l'assistenza tecnica viene fornita tramite il distributore. È possibile tuttavia richiedere l'assistenza tecnica diretta da parte degli esperti di VASCO.

Per ulteriori informazioni sulla nostra offerta di servizi di assistenza, consultare il sito www.vasco.com/support.

Soluzioni di autenticazione VASCO per tutte le esigenze

Per le aziende di piccola e media dimensione

■ Pacchetto DIGIPASS per l'autenticazione remota

Una soluzione predefinita per l'accesso remoto sicuro comprensiva di software server e sistemi di autenticazione degli utenti finali.

Per aziende di tutte le dimensioni

Back-end

■ aXsGUARD Gatekeeper

Soluzione UTM completa per l'accesso remoto protetto.

■ Server di autenticazione IDENTIKEY

Server di autenticazione centralizzato disponibile in quattro diverse offerte per l'uso aziendale.

■ Dispositivo IDENTIKEY

Dispositivo di autenticazione dedicato per aziende di media e grande dimensione.

■ IDENTIKEY Federation Server

Piattaforma di gestione dell'accesso e dell'identità per convalidare le credenziali degli utenti su diverse applicazioni e reti diffuse.

■ DIGIPASS as a Service

Autenticazione basata sul cloud in un'offerta di servizio gestito.

Per gli utenti

■ Famiglia DIGIPASS

Gamma di oltre 100 dispositivi di autenticazione tra cui dispositivi a un pulsante e tastiere PIN, lettori di schede e soluzioni basate su software.

■ DIGIPASS CertiID™

Soluzione PKI di VASCO basata su client per la crittografia di file e dischi e per la firma di documenti, e-mail e transazioni.



SEAL

SEAL: PER ESSERE INFORMATI E AGGIORNATI

Aggiornamenti sulle ultime tendenze in fatto di sicurezza

Quasi ogni giorno emergono dei nuovi tipi di attacchi online. Per i professionisti della sicurezza IT è quindi fondamentale rimanere informati e aggiornati sulle ultime tendenze. In qualità di azienda leader nel settore della sicurezza Internet, VASCO considera suo dovere condividere attivamente con clienti, partner, distributori, rivenditori e con chiunque richieda la sua consulenza le informazioni sulle tendenze presenti e future in fatto di sicurezza IT e sugli schemi di frode online.

Piattaforma Security Experts Academy & e-Learning (SEAL) di VASCO

SEAL è la comunità mondiale di VASCO dedicata ai professionisti della sicurezza. L'offerta formativa SEAL è composta da argomenti di sicurezza IT generici e da proposte di formazione sui prodotti VASCO, preziose per le persone che desiderano costruirsi una carriera nel settore della sicurezza delle informazioni. Tramite la nostra offerta di formazione in classe, e-learning o formazione tramite DVD e forum, la proposta SEAL di VASCO consente di:

- Diventare un ingegnere certificato VASCO
- Essere aggiornati sulle ultime tendenze in fatto di sicurezza
- Sviluppare nuove competenze in fatto di sicurezza IT
- Accedere a una comunità con conoscenze approfondite in fatto di sicurezza IT
- Scambiare informazioni con i colleghi

Se volete aumentare le vostre conoscenze nel campo della sicurezza IT, iscrivetevi a VASCO SEAL e diventerete dei professionisti in fatto di sicurezza. I corsi SEAL sono consigliati per addetti alle vendite, manager dei prodotti, ingegneri addetti all'assistenza, ingegneri sul campo e consulenti in fatto di sicurezza.

Offerta SEAL

La proposta SEAL di VASCO è composta dai seguenti elementi:

- E-learning: oltre 120 ore di formazione sulla sicurezza tramite corsi sul web o in DVD.
- Formazione in classe con gli esperti della sicurezza VASCO.
- Certificazione VASCO: la formazione SEAL offre ai professionisti della sicurezza IT l'opportunità di diventare ingegneri certificati VASCO.
- Centri di formazione autorizzati VASCO: formazione da parte dei partner VASCO.
- Programmi junior: programmi per tirocinanti e borse di studio per neo-diplomati o neo-laureati.

Per ulteriori informazioni, consultare il sito www.vasco.com/training.



Storie di successo



Stageco costruisce una rete ridondante per le sue filiali utilizzando aXsGUARD Gatekeeper

Stageco è un'azienda internazionale che produce e progetta attrezzature per lo spettacolo standardizzate e personalizzate, tra cui le strutture utilizzate dagli artisti più famosi. Il gruppo ha nove sedi in tutto il mondo e deve monitorare i processi logistici di ogni evento. Esasperata da connessioni VPN lente e dalle continue interruzioni, l'azienda decide di creare una rete ridondante tramite i cosiddetti e-tunnel con VASCO aXsGUARD Gatekeeper.

Installando un secondo dispositivo aXsGUARD, Stageco è riuscita a creare un e-tunnel e a garantire una connessione veloce, stabile e ridondante alla rete, nonché un database del magazzino per le sedi remote. La soluzione consente l'accesso singolo e pertanto permette una modalità di lavoro molto più efficiente e semplice.

STAGECO
BELGIUM N.V.



Galapagos protegge la proprietà aziendale, la rete e la VPN con aXsGUARD Gatekeeper.

Galapagos è un'azienda Europea che opera nel settore delle biotecnologie, europea specializzata nella scoperta e nello sviluppo di farmaci per la cura delle malattie osteoarticolari. Per proteggere i dati aziendali fondamentali, l'azienda voleva implementare una soluzione di sicurezza completa che proteggesse la rete, la rete VPN, il sito web e il traffico e-mail.

Stabilità e assistenza erano fattori decisivi alla luce delle limitate risorse IT di Galapagos. Anche l'accesso remoto alla rete aziendale era una necessità primaria. aXsGUARD Gatekeeper è stata una delle poche soluzioni che poteva essere completamente integrata nell'infrastruttura aziendale preesistente. Da quando è stato implementato aXsGUARD Gatekeeper, le interruzioni si sono azzerate e l'assistenza fornita è eccellente. I dipendenti e i ricercatori esterni Galapagos possono accedere alla rete aziendale in modo protetto da qualunque località del mondo.

Galapagos

Global Radio protegge l'accesso remoto e sviluppa una politica di sicurezza a lungo termine con un'autenticazione articolata



Global Radio è il più grande gruppo radiofonico commerciale del Regno Unito e comprende diverse radio commerciali famose. Con oltre 50 località in tutto il paese e oltre 18,5 milioni di ascoltatori, Global Radio copre quasi tutti i generi e le aree geografiche del Regno Unito. Quando cercava una efficace soluzione di autenticazione per l'accesso remoto protetto degli editor dei contenuti del sito web, Global Radio ha scelto VASCO DIGIPASS for Mobile in combinazione con Virtual DIGIPASS, DIGIPASS GO 3 e il server di autenticazione IDENTIKEY Enterprise Edition come back-end. Le soluzioni VASCO non solo hanno permesso di risolvere i problemi di sicurezza attuali, ma si sono anche inserite in modo perfetto nei piani di sviluppo della sicurezza a lungo termine dell'azienda.

global
thisisglobal.com



PER UNA MAGGIORE FIDUCIA DEI CLIENTI.

UNO STOP ALLE MINACCE ALLA SICUREZZA.

La sicurezza come vantaggio sulla concorrenza

La sicurezza è una preoccupazione importante per tutti i fornitori di applicazioni e per gli utenti; soprattutto da quando le applicazioni sono diventate sempre più accessibili tramite le reti Internet e i dispositivi mobili.

La maggior parte delle applicazioni online sono protette per impostazione predefinita da un nome utente e da una password statica. Le password statiche, tuttavia, possono essere facilmente intercettate e non sono più in grado di offrire una protezione sufficiente.

I fornitori di applicazioni vogliono proteggere i dati contenuti nell'applicazione e di conseguenza i loro clienti. Per questo, se vogliono conquistare e mantenere la fiducia dei clienti ed evitare perdite di credibilità e di introiti, devono poter risolvere i problemi di sicurezza e prendere delle contromisure contro le frodi e i furti di dati.

Sicurezza integrata

Le soluzioni di forte articolata VASCO sono pensate per risolvere i problemi di sicurezza legati alle applicazioni online e per contrastare le frodi e i diversi attacchi senza ridurre la semplicità d'uso. Le soluzioni comprendono modalità di autenticazione attiva e passiva e possono basarsi sull'hardware, sul software o sui dispositivi mobili. È possibile applicare l'autenticazione forte a qualsiasi tipo di applicazione online, come ad esempio quelle per l'intermediazione online, le assicurazioni, l'e-commerce, i giochi online, le applicazioni sanitarie online, le applicazioni CRM, ERP e buste paga, i servizi SaaS e molto altro ancora.

Le soluzioni di autenticazione back-end VASCO consentono ai fornitori di applicazioni online di integrare l'autenticazione articolata e la protezione delle licenze direttamente all'interno dell'applicazione. Sono quindi una soluzione ideale per qualsiasi fornitore che intende acquisire e gestire milioni di utenti.

Soluzioni di autenticazione VASCO per tutte le esigenze

Protezione licenze DIGIPASS

Contrasta la perdita di introiti e le potenziali minacce alla sicurezza dovute alla condivisione di account e password.

Back-end

Controllor VACMAN

Tecnologia di autenticazione principale di VASCO, adatta a grandi implementazioni per molte applicazioni destinate ai clienti di diversi mercati verticali: giochi online, e-commerce, CRM, ERP, portali web ecc.

Server di autenticazione IDENTIKEY

Server di autenticazione centralizzato per migliorare la sicurezza delle applicazioni web.

IDENTIKEY Federation Server

Piattaforma di gestione dell'accesso e dell'identità per convalidare le credenziali degli utenti su diverse applicazioni e reti diffuse.

DIGIPASS as a Service

Autenticazione basata sul cloud in un'offerta di servizio gestito.

Per gli utenti

Famiglia DIGIPASS

Gamma di oltre 100 dispositivi di autenticazione tra cui dispositivi a un pulsante e tastiere PIN, lettori di schede e soluzioni basate su software.

DIGIPASS CertiID™

Soluzione PKI di VASCO basata su client per la crittografia di file e dischi e per la firma di documenti, e-mail e transazioni.



FOCALIZZAZIONE SULL'ATTIVITÀ AZIENDALE PRINCIPALE.

AUTENTICAZIONE DEI FORNITORI IN OUTSOURCING.

Il trionfo del cloud computing

Il cloud computing è la nuova tendenza e dominerà il paesaggio IT per i prossimi anni. Più flessibilità, più scalabilità e meno costi. Gli argomenti a favore del cloud computing sono difficili da contrastare.

VASCO offre il sistema DIGIPASS as a Service, un modello di autenticazione completamente in outsourcing. Il modello è stato progettato per i fornitori di servizi applicativi che desiderano aggiungere un'autenticazione articolata per proteggere contenuti, dati e applicazioni.

DIGIPASS as a Service risolve diversi problemi solitamente associati all'implementazione di una soluzione di autenticazione a due fattori. L'integrazione dell'autenticazione forte potrebbe richiedere delle modifiche all'infrastruttura. Inoltre, l'implementazione dell'autenticazione a due fattori su un numero elevato di utenti finali potrebbe essere considerata costosa e dispendiosa in termini di tempo. Carichi logistici, portabilità dei dispositivi di autenticazione, autenticatori distinti per le diverse applicazioni, installazione di software sul PC dell'utente finale, tutta la relativa amministrazione... i problemi sono molti.

Autenticazione dalla A alla Z

DIGIPASS as a Service va oltre queste preoccupazioni: l'autenticazione diventa un costo di esercizio anziché di un costo di capitale; in questo modo il costo dell'implementazione si abbassa, come pure il costo totale di possesso. VASCO si occupa dell'intero processo di autenticazione: dalla distribuzione e dall'amministrazione fino all'autenticazione dei dispositivi degli utenti finali.

Inoltre, con i dispositivi VASCO DIGIPASS Plus, il problema di autenticatori distinti per le diverse applicazioni appartiene al passato. I dispositivi DIGIPASS Plus sono dotati di una seconda identità, che consente agli utenti finali di utilizzare un dispositivo DIGIPASS per più applicazioni. Con la strategia VASCO DESS siamo in grado di mettere l'autenticazione a disposizione di chiunque. DIGIPASS as a Service consente alle organizzazioni e ai fornitori di applicazioni di focalizzarsi sulle loro specifiche competenze, senza preoccuparsi dei problemi di sicurezza.

MYDIGIPASS.COM

MYDIGIPASS.COM è una piattaforma online che consente ai proprietari delle applicazioni web una gestione semplice delle password e allo stesso tempo di aggiungere un ulteriore livello di sicurezza alla procedura di accesso. VASCO consente ai proprietari di siti web di integrare liberamente l'autenticazione articolata sul loro sito tramite password DIGIPASS usa e getta, in modo che gli utenti finali possano accedere in modo protetto ai loro servizi e ai loro contenuti.

I proprietari di siti web possono aumentare la fiducia dei clienti fornendo un accesso singolo a tutte le applicazioni collegate alla piattaforma. Inoltre, possono ridurre i costi di back-office e di assistenza eliminando i costi associati alla gestione delle password.

Gli utenti finali, a loro volta, possono accedere in modo comodo e sicuro alle loro applicazioni tramite il portale MYDIGIPASS.COM sfruttando la tecnologia DIGIPASS di VASCO. Per generare una password usa e getta di accesso alla piattaforma, possono usare uno dei milioni di DIGIPASS pronti a essere attivati oppure scaricare gratuitamente un client per dispositivi mobili da MYDIGIPASS.COM.



MYDIGIPASS.COM™





CONVENIENTE. INDIPENDENTE DALLA PIATTAFORMA. PROTEZIONE ELEVATA

Autenticazione della comunità online

L'integrazione di DIGIPASS e le soluzioni OEM sono la risposta VASCO alla continua evoluzione del mercato dell'autenticazione. È una prova dell'impegno di VASCO per trovare dei modi più comodi, portatili e convenienti per proteggere la comunità online. VASCO si impegna a sviluppare delle soluzioni di autenticazione in grado di funzionare su qualsiasi piattaforma e che siano adeguate per proteggere qualsiasi applicazione.

Soluzioni OEM

VASCO sviluppa soluzioni di sicurezza pratiche che bilanciano sicurezza e comodità per tutti i clienti. La famiglia DIGIPASS di VASCO è stata progettata per funzionare su una singola infrastruttura e tutti i diversi fattori che la costituiscono possono interagire tra loro.

Questo consente ai partner VASCO di aggiungere l'autenticazione forte alla loro offerta senza investimenti cospicui o interruzioni della loro attività aziendale. Poiché l'autenticazione diventa un elemento cruciale in tutte le infrastrutture di sicurezza, la gamma di prodotti VASCO fornisce alle organizzazioni un vantaggio unico sulla concorrenza che può contribuire ad aumentare la quota di mercato e le entrate. Poiché le nostre soluzioni sono versatili, possono adattarsi semplicemente alle esigenze di qualsiasi cliente.

Soluzioni di sicurezza integrate

La missione di VASCO per le DIGIPASS Embedded Security Solutions (DESS) è quella di attivare la tecnologia DIGIPASS su dispositivi e applicazioni del cliente: qualunque essi siano. La tecnologia DIGIPASS pronta all'attivazione viene integrata nei prodotti delle aziende leader del settore e consente a chiunque di avere l'autenticazione a portata di mano.

Questo processo cambia il paradigma dell'autenticazione: invece di distribuire dei dispositivi di sicurezza agli utenti finali, VASCO fornisce quel livello di protezione a un dispositivo già in possesso dell'utente.

Le DIGIPASS Embedded Security Solutions sfidano la convinzione che a una maggiore comodità per l'utente corrispondono automaticamente un minore costo associato e una minore protezione. Con l'integrazione in una infrastruttura già esistente, i costi sono naturalmente inferiori. L'equazione viene quindi modificata: da un modello in cui si sacrifica la sicurezza in favore del costo e della comodità si passa a un modello in cui la sicurezza diventa la base di tutte le applicazioni online.

Le opportunità della sicurezza DIGIPASS integrata comprendono:

- Piattaforme per computer
- Piattaforme mobili
- Smart card e credenziali di sicurezza esistenti
- USB/SD/MMC/SIM o altri dispositivi o schede di memoria
- Software di sicurezza

La tecnologia DIGIPASS pronta all'attivazione viene integrata nei prodotti delle aziende leader del settore e consente a chiunque di avere l'autenticazione a portata di mano.



HARIBO Italia protegge le informazioni riservate del suo programma CRM con DIGIPASS e IDENTIKEY

HARIBO Italia, la filiale italiana della multinazionale HARIBO, è l'azienda leader in Italia per la fornitura di gomme da masticare e gelatine. Per gestire i contatti e le informazioni di vendita, gli agenti dell'azienda utilizzano un programma CRM nel cloud. La semplicità di uso è stato un elemento fondamentale per questa scelta. Gli agenti di vendita HARIBO non devono percepire la soluzione come un ostacolo. Altri fattori decisionali importanti sono stati il basso costo di implementazione e il basso impatto sull'infrastruttura IT esistente.

HARIBO ha scelto la tecnologia DIGIPASS di VASCO unita a un server di autenticazione IDENTIKEY. I cinquantacinque agenti di vendita dell'azienda, in movimento sull'intero territorio italiano, possono ora utilizzare DIGIPASS GO 6 unito a una soluzione Barracuda SSL-VPN e accedere in remoto e in modo sicuro al programma CRM.



HARIBO



Una nota azienda di giochi online si affida alle soluzioni VASCO per proteggere gli account dei suoi utenti

Per proteggere gli account di gioco degli utenti finali dall'intrusione, una nota azienda di giochi online ha implementato una soluzione in grado di elaborare le richieste di accesso di oltre centomila giocatori, pur mantenendo la semplicità di utilizzo da parte degli utenti. La soluzione deve riflettere l'identità dell'azienda e quindi essere in grado di integrare loghi e immagini per aumentare il riconoscimento del marchio.

DIGIPASS GO 6 in combinazione con il controller VACMAN offre un'autenticazione articolata che protegge l'accesso remoto al gioco senza la necessità di installare software sul PC. DIGIPASS GO 6 è semplice da utilizzare, è portatile e può essere utilizzato come strumento di marketing poiché ha un telaio completamente personalizzabile, in grado di ospitare il marchio dell'azienda.



Cardinal IP: un'applicazione SaaS per gestire la proprietà intellettuale protetta da DIGIPASS

Cardinal IP è un leader mondiale nel campo della ricerca e dei brevetti. La riservatezza e la protezione sono fattori estremamente importanti quando si devono proteggere i dati di proprietà intellettuale e le ricerche. Cardinal IP doveva implementare una tecnologia conveniente e scalabile per proteggere l'accesso alla rete extranet aziendale e alla sua soluzione SaaS "IP Dashboard"; il livello di sicurezza doveva essere conforme ai requisiti FISMA. La soluzione di sicurezza doveva essere completamente integrata nelle applicazioni basate sul web e create internamente da Cardinal IP e nella rete extranet aziendale; doveva inoltre essere facilmente gestibile e avere un livello elevato di accettazione da parte degli utenti.

Le tecnologie VACMAN e DIGIPASS sono state integrate nelle applicazioni web Cardinal IP e nella rete extranet per mezzo di uno strumento SQL Server e di ASP.NET. Questo garantisce che tutti i dipendenti e i clienti che accedono alla rete aziendale e alle applicazioni siano adeguatamente autenticati. Poiché non è stato necessario installare alcun software aggiuntivo sui computer degli utenti finali, la soluzione di autenticazione VASCO è risultata essere economicamente conveniente ed è stata accettata rapidamente da dipendenti e clienti di Cardinal IP.





CREARE FIDUCIA NEI CITTADINI.

LAVORARE IN MODO PIÙ EFFICIENTE.

Con l'esplosione dell'e-government, la sicurezza diventa essenziale

Le amministrazioni pubbliche di tutto il mondo adottano strategie di e-government per offrire ai cittadini una gamma più ampia di servizi pubblici. L'implementazione dell'e-government ha dei notevoli vantaggi: le procedure si semplificano, la burocrazia si riduce, i servizi diventano accessibili al di fuori dell'orario d'ufficio; il risultato di tutto questo è una modalità di trasmissione di informazioni e servizi più economica, più efficiente e più comoda.

Allo stesso tempo, però, le preoccupazioni sulla privacy e sui dati sono aumentate. I cittadini devono essere sicuri che i dati e le credenziali siano protetti e che possano essere scambiati in un ambiente protetto.

Le amministrazioni devono garantire che le applicazioni e i dati fondamentali legati alla sicurezza nazionale, ai servizi pubblici, alle imposte, alle entrate, alla sanità ecc. siano adeguatamente protetti. Devono essere vigili e prendere tutte le misure di sicurezza necessarie per vincere queste sfide. Inoltre, le applicazioni e i dati degli enti pubblici devono rispettare le regole di conformità previste dagli standard internazionali per l'accesso protetto online a sistemi ed enti amministrativi.

Le tecnologie OTP e PKI garantiscono la sicurezza

Le soluzioni di autenticazione a due fattori VASCO forniscono un'autenticazione dell'utente finale in grado di garantire l'accesso remoto, eliminando le debolezze intrinseche delle password statiche. Le nostre soluzioni PKI offrono ad enti e istituti pubblici un ambiente PKI protetto per le transazioni e la firma online dei documenti garantendo l'integrità e il non ripudio dei dati.

I lettori di carte di identità elettronica VASCO consentono ai cittadini di accedere alle applicazioni online e di richiedere i documenti online in qualsiasi momento. Le aziende possono usare i lettori di carte eID VASCO per collegare le applicazioni a un ID specifico garantendo l'accesso autorizzato.

I lettori di carte eID DIGIPASS sono disponibili nelle modalità collegata, collegabile e non collegata. I dispositivi non collegati leggono i dati contenuti nel chip della carta e generano degli OTP per l'accesso sicuro alle applicazioni, all'e-mail o alle reti. I lettori di carte collegati possono essere collegati a specifiche applicazioni e consentire agli utenti di accedere all'autenticazione e ai certificati di firma archiviati sul chip.

Soluzioni di autenticazione VASCO per tutte le esigenze

Back-end

- **Controller VACMAN**
Tecnologia di autenticazione principale di VASCO, adatta a implementazioni con un elevato numero di utenti finali.
- **Server di autenticazione IDENTIKEY**
Server di autenticazione centralizzato che facilita l'accesso remoto e la sicurezza delle applicazioni.
- **Dispositivo IDENTIKEY**
Un dispositivo di autenticazione dedicato
- **aXsGUARD Gatekeeper**
Una soluzione UTM completa per l'accesso remoto protetto.

Per gli utenti

- **Famiglia DIGIPASS**
Gamma di oltre 100 dispositivi di autenticazione tra cui dispositivi a un pulsante e tastiere PIN, lettori di schede e soluzioni basate su software.
- **Lettori di carte DIGIPASS eID card**
Lettori di carte di identità elettroniche disponibili nelle modalità collegata, collegabile e non collegata.
- **DIGIPASS CertiID™**
Soluzione PKI di VASCO basata su client per una autenticazione articolata dell'utente, crittografia di file e dischi, scambio di e-mail protetto e firma di transazioni e documenti.



PZ Vlas dà alla sicurezza la massima priorità utilizzando lettore eID VASCO DIGIPASS 820

Nell'era digitale, il Belgio è stato uno dei primi paesi a implementare e distribuire le carte di identità elettroniche ai propri cittadini. Dati come il nome del cittadino, il numero di carta e la foto sono stampati su queste carte eID, mentre altri dati come l'indirizzo sono archiviati sul chip della carta stessa. Gli agenti di polizia in servizio devono essere in grado di leggere l'indirizzo dei cittadini archiviato sul chip della carta. Il lettore e-ID deve essere portatile e di facile utilizzo per gli agenti in servizio. Deve essere adatto a tutte le unità: auto, moto, bici e a piedi.

Il lettore eID VASCO DIGIPASS 820 può essere comodamente riposto nelle tasche dell'uniforme grazie al suo design particolarmente piatto. Può inoltre essere utilizzato in tutte le condizioni climatiche grazie alla struttura a prova di urti e alla protezione da polvere e liquidi integrata nel tastierino in gomma. L'elevata facilità di utilizzo permette agli agenti di verificare l'indirizzo dei cittadini nel giro di pochi secondi.



POLITIEZONE VLAS

CD&V consente al suo personale e ai volontari di accedere in remoto alla sua rete in modo protetto grazie alla tecnologia DIGIPASS

CD&V è un partito politico belga che, per la sua organizzazione, aveva bisogno di una soluzione di accesso remoto protetta per consentire al personale di accedere alla rete ovunque e in qualsiasi momento. Il partito voleva un metodo di accesso alla sua rete più sicuro di una semplice password statica, così da poter proteggere i dati riservati e impedire l'accesso non autorizzato. Era però essenziale un sistema facilmente accettato dagli utenti. I dipendenti non dovevano percepire la soluzione come un ostacolo. Inoltre la soluzione non doveva causare dei ritardi nei trasferimenti di dati e doveva poter essere gestita semplicemente dagli addetti IT del partito.

La tecnologia DIGIPASS di VASCO e il server di autenticazione IDENTIKEY hanno permesso a CD&V di proteggere la soluzione Citrix XenApp in modo molto poco oneroso dal punto di vista economico. Grazie all'interfaccia di amministrazione basata sul web del server di autenticazione IDENTIKEY, la gestione del processo di autenticazione è semplicissima. L'autenticatore con un solo pulsante è molto facile da usare ed è stato subito accettato dai dipendenti. I dipendenti possono ora accedere in modo sicuro ai dati riservati ovunque si trovino e in qualunque momento grazie al DIGIPASS GO 6.



Il Dorset County Council protegge i dati riservati e la rete interna tramite una combinazione di crittografia PKI e password dinamiche

Il Dorset County Council è un ente amministrativo elettivo alla ricerca di una soluzione di autenticazione per proteggere l'accesso remoto alla rete dei dipendenti e i dati riservati archiviati sui laptop.

VASCO DIGIPASS GO 3 fornisce ai dipendenti in movimento dell'ente una soluzione di accesso remoto sicura. Implementando DIGIPASS 860 con funzionalità PKI, gli utenti dei laptop sono in grado di accedere in remoto alla rete dell'ente tramite password dinamiche generate che salvaguardano i dati critici archiviati nei laptop grazie alla crittografia degli hard disk. Le soluzioni DIGIPASS sono completamente compatibili con l'infrastruttura back-end esistente, che consente al Dorset County Council di implementare l'autenticazione a due fattori con il minor costo per il possessore.

