



- • • Encryption algorithms • •
- Cryptographic software • • •
- Digital rights management • • •
- Link encryptor • • • Integration •
- • HSM • • • Database encryption
- • • Vulnerability Assessment • •
- Penetration Test • • • VPN • • •
- Firewall • • • Security Information
and Event Management • •
- Professional Services • • •
- Implementation • • • Customization
- • • Training • • • Consulting
Services • • •

Presente sul mercato italiano da oltre dieci anni, Intrinsic è un'azienda di Information Technology che opera nell'ambito della progettazione di complesse soluzioni crittografiche per la protezione e l'integrità dei dati, cifratura di database, sistemi anticontraffazione, strong authentication e più in generale attività nell'ambito della network security.

La divisione R&D di Intrinsic è in grado di sviluppare soluzioni personalizzate nell'ambito della firma digitale, realizzare librerie crittografiche e fornire alle principali aziende italiane e alla Pubblica Amministrazione consulenza strategica per migliorare la sicurezza delle infrastrutture ICT.

Il team dei tecnici Intrinsic vanta un'esperienza di lavoro di gruppo considerevole, maturata in tanti anni di attività, a favore delle principali aziende italiane nel settore dell'e-Government, Telco e Utilities, Sanità, Difesa, Trasporti e Logistica, Banche e Assicurazioni. L'offerta Intrinsic copre le esigenze di aree di mercato con soluzioni innovative finalizzate alla cifratura di reti e sistemi, soluzioni anti-malware, VPN-SSL, Firewall, dispositivi di Intrusion Prevention & Detection e soluzioni di Security Information and Event Management (SIEM).

Intrinsic è inoltre in grado di erogare servizi professionali nell'ambito della sicurezza delle reti e dei sistemi, attività di Vulnerability Assessment, Penetration Test, nonché procedure di setup e tuning di dispositivi di networking.

Security Services

1. Statistiche anonime sugli utenti
2. Servizi di strong authentication
3. Ampliamento di un sistema per la multifirma remota
4. Protezione del software
5. Cifratura di database
6. Penetration Test
7. Vulnerability Assessment
8. Installazione e setup di soluzioni di security
9. Technological Partner

- • • Encryption algorithms
- • • Cryptographic software
- • • HSM
- • • Database encryption

Statistiche anonime sugli utenti

Progettazione di un sistema di anonimizzazione dei dati per effettuare statistiche sugli utenti di una Telco che desidera raccogliere informazioni su larga scala, nel rispetto della privacy. La necessità del cliente è quella di mettersi nelle condizioni di non poter individuare le singole persone ma fare solamente conteggi con etichette fittizie. Questo permette ai gestori di indirizzare i propri servizi verso quelle linee di mercato che l'utenza predilige e concentrarsi sul miglioramento della loro qualità senza venire a conoscenza delle abitudini dei singoli.

La realizzazione di questo progetto prevede l'impiego di moduli hardware per la sicurezza (HSM) che, oltre alla protezione delle chiavi crittografiche, consentono l'esecuzione di algoritmi personalizzati al loro interno. E' importante infatti che le procedure di anonimizzazione siano eseguite all'interno di un perimetro sicuro dove il codice e i dati parziali non sono accessibili. Solo il risultato finale viene reso noto all'applicativo esterno che raccoglie e gestisce le informazioni provenienti dalla rete.

- • • Encryption algorithms
- • • Cryptographic software
- • • Link encryptor
- • • Integration

Servizi di strong authentication

Gestione dell'accesso alle risorse di un grande cliente attraverso sistemi VPN-SSL supportati dalla doppia autenticazione offerta dai token hardware. Gli utenti, quando si trovano in trasferta, possono accedere ai servizi della rete aziendale utilizzando una piccola chiavetta (delle dimensioni di un accendino) che permette al sistema centrale di riconoscere chi si sta connettendo e quali autorizzazioni possiede. A differenza dei sistemi basati su password, questa infrastruttura offre un grado di sicurezza molto maggiore. Per ogni connessione infatti è necessario non solo l'uso delle proprie credenziali, come nei sistemi tradizionali, ma anche la presenza fisica del token, il quale non può essere in alcun modo duplicato o bypassato. L'utente è quindi sicuro che, se il token rimane in suo possesso, un accesso abusivo a suo nome non può avvenire.

- • • Encryption algorithms
- • • Cryptographic software
- • • Integration
- • • HSM
- • • Customization
- • • Consulting Services

Ampliamento di un sistema per la multifirma remota

Reingegnerizzazione di una interfaccia di comunicazione (e relativo substrato logico) di un modulo di sicurezza per la firma digitale (HSM) in modo che quest'ultimo possa gestire un numero arbitrario di chiavi, appoggiando il proprio storage su un database esterno. In questo modo viene resa possibile la firma remota su grandi realtà che superano il milione di utenti, mantenendo gli applicativi già disponibili. Questo permette un notevole risparmio nella manutenzione del codice da parte dei programmatori che gestiscono l'infrastruttura di firma digitale, offrendo al tempo stesso un sistema dalla scalabilità quasi illimitata.

- • • Encryption algorithms
- • • Cryptographic software
- • • Integration
- • • HSM
- • • Implementation
- • • Customization
- • • Consulting Services

Protezione del software

Design di algoritmi crittografici per la firma corta, utilizzati per il licensing e la protezione del software. Attraverso una combinazione di librerie software e dispositivi hardware, vengono realizzati sistemi che permettono alle software house di impedire la copia abusiva dei propri applicativi senza richiedere all'utente finale l'esecuzione di procedure lunghe e complesse.

Da una parte il dongle subordina l'esecuzione del programma alla sua presenza nella porta USB del PC, dall'altra la crittografia a firma corta permette di regolare le feature aggiuntive del prodotto. Per esempio è possibile controllare la scadenza delle licenze o l'attivazione di funzionalità particolari attraverso un codice alfanumerico di 20-25 caratteri, che può essere agevolmente fornito dalla software house anche per telefono o stampandolo sull'etichetta del CD.

- • • Encryption algorithms
- • • Cryptographic software
- • • Integration
- • • HSM
- • • Database encryption

Progettazione di sistemi per la cifratura di database che rendono trasparente l'accesso ai dati per gli utenti autorizzati. Uno dei principali problemi che si trovano ad affrontare le grandi aziende è quello della protezione dati del proprio database, poiché esso contiene spesso informazioni di vitale importanza. Al tempo stesso vi è quasi sempre la necessità di mantenere inalterati gli applicativi in uso per l'accesso ai dati, in quanto oltre a permettere un risparmio sui costi, consentono all'utente di continuare ad usare procedure conosciute ed affidabili.

Per questa ragione l'utilizzo di appliance come Datasecure, in congiunzione ad una analisi del contesto specifico da parte di un nostro specialista, risulta essere un ottimo investimento per la protezione dei propri dati in modo trasparente e sicuro.

- • • Vulnerability Assessment
- • • Penetration Test
- • • Professional Services
- • • Implementation
- • • Consulting Services

Penetration Test

Il servizio prevede l'analisi della sicurezza del perimetro esterno della rete del cliente. In particolare vengono analizzati tutti gli host attivi alla ricerca di server configurati non correttamente, inoltre vengono ricercate vulnerabilità note, utilizzate in genere dagli hacker per la compromissione dei sistemi. Nella fase preliminare del servizio, il cliente può decidere se includere o meno eventuali attacchi di tipo Denial Of Service o di Brute Force. Al termine dell'attività viene prodotto un Security Report su cui vengono evidenziate le vulnerabilità riscontrate nella configurazione della rete e i suggerimenti per renderla più sicura. Questo servizio viene condotto remotamente dalla sede di Intrinsic.

- • • Vulnerability Assessment
- • • Penetration Test
- • • Professional Services
- • • Implementation
- • • Consulting Services

Vulnerability Assessment

Il servizio prevede l'analisi dello stato della sicurezza della rete interna del cliente. Facendo seguito alla presa visione della realtà da esaminare, viene effettuata una scansione dettagliata di tutta la rete per rilevare gli host attivi, i loro sistemi operativi, relativi servizi e possibili vulnerabilità. Durante l'assessment inoltre vengono analizzate eventuali reti wireless presenti sulla rete del cliente e le configurazioni dei sistemi di sicurezza installati. Al termine dell'attività di vulnerability assessment viene generato un Security Report contenente nel dettaglio le vulnerabilità e i problemi riscontrati. Vengono inoltre fornite istruzioni su come modificare le configurazioni dei sistemi al fine di ovviare agli inconvenienti rilevati.

- • • Professional Services
- • • Implementation
- • • Customization
- • • Training
- • • Consulting Services

Installazione e setup di soluzioni di networking e security

In ogni progetto legato alla sicurezza, la fase di implementazione è critica e importante quanto la progettazione. Data la natura altamente specialistica di alcuni dei prodotti nell'ambito del networking e della security, può accadere che il cliente finale non possieda le figure professionali più idonee a curarne il deployment e a configurare correttamente il sistema. Intrinsic offre quindi un servizio di installazione e configurazione per tutte le soluzioni commercializzate, grazie alla presenza di personale qualificato in grado di affiancare il cliente e seguire il progetto a partire dalla progettazione fino al deployment e al fine-tuning, in modo da assicurare un utilizzo ottimale della soluzione.

• • • I nostri technological partner

Technological Partner

CREDANT 

F-Secure 

JUNIPER
NETWORKS

 **Network Critical**

 **Q Labs**

 **SafeNet**

SOURCEfire[®]

 **Symantec**

TECTIA

THALES

 **VASCO**

 **WatchGuard**



Intrinsic
Viale Mentana, 29
I-43121 Parma

T. 0521-708866
F. 0521-776190

info@intrinsic.it
www.intrinsic.it