

Milano, 8 Novembre 2006

Spett.le

**Sipra S.p.A.**

Corso Unione Sovietica, 612/3D  
10135 Torino

Offerta n. 20061106.mb42

**Alla c. att.ne : Dott. Rino Zaccaria**

**Oggetto: Offerta per Soluzione di Smart Card e relativo sistema di gestione CMS**

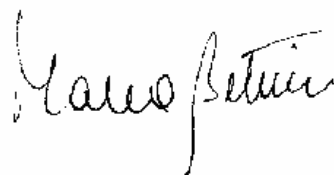
A seguito della Vostra gradita richiesta, Vi sottoponiamo la nostra migliore proposta per la soluzione in oggetto.

In attesa di un vostro gradito riscontro, vi porgiamo i nostri più cordiali saluti.

**Hacking Team Srl**

**Marco Bettini**

Key Account Manager



---

Hacking Team S.r.l.

Sede legale e Amministrativa: Via Freguglia Carlo, 2- 20122 Milano

Sede operativa: Via della Moscova, 13 - 20121 Milano - Tel: +39.02.29060603

e-mail: [info@hackingteam.it](mailto:info@hackingteam.it) - web: <http://www.hackingteam.it> - Fax: +39.02.63118946

P.IVA: 03924730967 - Capitale Sociale: € 100.000,00 i.v.

N° Reg. Imprese / CF 03924730967 - N° R.E.A. 1712545

---

<b>Titolo documento:</b>	<b>Tipo documento:</b>	<b>Versione:</b>
Offerta per Sipra S.p.A. 20061106.mb42	Offerta	1.0

## **Offerta per la fornitura di soluzione di Smart Card con relativo sistema di gestione CMS**

<b>Data documento:</b> 8 Novembre 2006	<b>Autore:</b> Marco Bettini	<b>Revisore:</b> Valeriano Bedeschi	<b>Codice documento:</b> OFF-20061106.mb42	<b>Pagina:</b> 2 di 8
---	---------------------------------	--	---	--------------------------

<b>Titolo documento:</b>	<b>Tipo documento:</b>	<b>Versione:</b>
Offerta per Sipra S.p.A. 20061106.mb42	Offerta	1.0

## SOMMARIO

<b>STORIA DEL DOCUMENTO .....</b>	<b>4</b>
<b>1. OBIETTIVI.....</b>	<b>5</b>
<b>2. REQUISITI.....</b>	<b>5</b>
<b>2.1. STRONG AUTHENTICATION PER IL DOMINIO MICROSOFT WINDOWS2000.....</b>	<b>5</b>
<b>2.2. GESTIONE CENTRALIZZATA DELLE PROBLEMATICHE DI HELP DESK.....</b>	<b>5</b>
<b>2.3. ARCHITETTURA LOGICA.....</b>	<b>6</b>
<b>2.4. CERTIFICATION AUTHORITY .....</b>	<b>6</b>
<b>2.5. USER REPOSITORY LDAP (MS ACTIVE DIRECTORY).....</b>	<b>6</b>
<b>2.6. CMS DATABASE STORAGE .....</b>	<b>6</b>
<b>2.7. ACTIVIDENTITY CARD MANAGEMENT SYSTEM (CMS).....</b>	<b>6</b>
<b>2.8. ACTIVIDENTITY ACTIVCLIENT.....</b>	<b>7</b>
<b>2.9. CONSOLE DI AMMINISTRAZIONE .....</b>	<b>7</b>
<b>3. QUOTAZIONE PRODOTTI ACTIVIDENTITY.....</b>	<b>8</b>
<b>4. CONDIZIONI GENERALI.....</b>	<b>8</b>

Data documento: 8 Novembre 2006	Autore: Marco Bettini	Revisore: Valeriano Bedeschi	Codice documento: OFF-20061106.mb42	Pagina: 3 di 8
------------------------------------	--------------------------	---------------------------------	--	-------------------

<b>Titolo documento:</b>	<b>Tipo documento:</b>	<b>Versione:</b>
Offerta per Sipra S.p.A. 20061106.mb42	Offerta	1.0

## **STORIA DEL DOCUMENTO**

<b>Versione:</b>	<b>Data:</b>	<b>Modifiche effettuate:</b>
1.0	8 Novembre 2006	Emissione Offerta

Data documento: 8 Novembre 2006	Autore: Marco Bettini	Revisore: Valeriano Bedeschi	Codice documento: OFF-20061106.mb42	Pagina: 4 di 8
------------------------------------	--------------------------	---------------------------------	--	-------------------

<b>Titolo documento:</b>	<b>Tipo documento:</b>	<b>Versione:</b>
Offerta per Sipra S.p.A. 20061106.mb42	Offerta	1.0

## 1. OBIETTIVI

Le funzionalità che il sistema realizza sono le seguenti:

- strong authentication per il dominio Microsoft Windows2000;

A livello architetturale, il sistema si compone di tre elementi opportunamente integrati:

- una certification authority per l'emissione di certificati digitali X.509, che sono utilizzati dagli utenti per scopi di autenticazione e/o cifratura;
- un sistema di gestione del ciclo di vita dei certificati e dei dispositivi hardware sicuri (smart card o USB key) che permette di centralizzarne le operazioni di emissione, rinnovo, sostituzione e revoca; il sistema supporta inoltre le funzionalità di help desk (in modalità assistita o self service) per l'utente finale (procedure di sblocco della smart card, richiesta rinnovo o sostituzione, ecc.);
- un layer software lato client (installato sulle workstation degli utenti finali) per l'accesso ai dispositivi hardware sicuri da parte del sistema operativo e/o delle applicazioni.

## 2. REQUISITI

### 2.1. STRONG AUTHENTICATION PER IL DOMINIO MICROSOFT WINDOWS2000

Il sistema permette di automatizzare emissione, rinnovo e revoca di certificati digitali X.509 su smart card o token USB crittografici che possono essere utilizzati dagli utenti come credenziali di accesso al dominio. La validazione delle credenziali avviene tramite le procedure di autenticazione del sistema operativo Microsoft (PKI Logon).

### 2.2. GESTIONE CENTRALIZZATA DELLE PROBLEMATICHE DI HELP DESK

Il sistema implementa funzionalità di help desk a cui gli utenti finali possono accedere nei seguenti casi:

- smarrimento della smart card o USB key;
- temporanea indisponibilità di smart card o USB key;
- blocco della smart card o USB key.

Data documento: 8 Novembre 2006	Autore: Marco Bettini	Revisore: Valeriano Bedeschi	Codice documento: OFF-20061106.mb42	Pagina: 5 di 8
------------------------------------	--------------------------	---------------------------------	--	-------------------

<b>Titolo documento:</b>	<b>Tipo documento:</b>	<b>Versione:</b>
Offerta per Sipra S.p.A. 20061106.mb42	Offerta	1.0

I servizi di help desk sono fruibili secondo due diverse modalità:

- supporto telefonico: un operatore supporta l'utente finale nella risoluzione del problema, per mezzo di una opportuna interfaccia web.;
- self service: l'utente finale accede, mediante una workstation condivisa, ad un servizio on-line per la risoluzione del problema.

### **2.3. ARCHITETTURA LOGICA**

L'architettura logica del sistema di gestione delle credenziali prevede quattro componenti lato server (certification authority, user repository LDAP, ActiveIdentity CMS e CMS database) ed un componente lato client (ActiveIdentity ActiveClient).

### **2.4. CERTIFICATION AUTHORITY**

La certification authority (CA) emette certificati digitali X.509 che costituiscono le credenziali per l'accesso al dominio e l'accesso alle chiavi di cifratura utilizzate da EFS.

### **2.5. USER REPOSITORY LDAP (MS ACTIVE DIRECTORY)**

Il sistema di gestione delle credenziali utilizza come repository di utenze la Active Directory del dominio. Su tale directory sono pubblicati:

- certificato della certification authority;
- certificate revocation list (CRL) della certification authority;
- certificati emessi per gli utenti ed i computer appartenenti al dominio.

### **2.6. CMS DATABASE STORAGE**

Il sistema di gestione delle credenziali utilizza un database MS SQL Server Enterprise Ed..

Tale database conserva le informazioni di stato del sistema relative a:

- assegnamento dei dispositivi crittografici (smart card e USB key) agli utenti;
- stato dei dispositivi;
- stato delle credenziali (certificati) presenti sui dispositivi crittografici;
- configurazione del CMS (si veda il successivo sottoparagrafo);
- jogging e auditing.

### **2.7. ACTIVIDENTITY CARD MANAGEMENT SYSTEM (CMS)**

ActiveIdentity Card Management System è la tecnologia con cui utilizzata per implementare la logica di gestione dei dispositivi crittografici e delle credenziali memorizzate su di essi. E' costituito da

Data documento: 8 Novembre 2006	Autore: Marco Bettini	Revisore: Valeriano Bedeschi	Codice documento: OFF-20061106.mb42	Pagina: 6 di 8
------------------------------------	--------------------------	---------------------------------	--	-------------------

<b>Titolo documento:</b>	<b>Tipo documento:</b>	<b>Versione:</b>
Offerta per Sipra S.p.A. 20061106.mb42	Offerta	1.0

tre applicazioni web (portal server, card content server, audit server) che realizzano rispettivamente le interfacce grafiche per gli amministratori e per gli utenti finali, la gestione dello stato dei dispositivi crittografici e le funzionalità di jogging e auditing.

## **2.8. ACTIVIDENTITY ACTIVCLIENT**

E' la componente lato client del sistema di gestione delle credenziali, responsabile dell'interfacciamento fra i dispositivi hardware crittografici in possesso degli utenti finali e le loro workstation. Dal punto di vista architetturale, il lato client della soluzione può essere diviso in due moduli:

- una interfaccia grafica per l'utente finale che permette di visualizzare informazioni relative al contenuto dei dispositivi, cambiare il PIN di sblocco degli stessi ed effettuare operazioni di diagnostica e troubleshooting (per utenti avanzati);
- una serie di librerie per l'interfacciamento fra applicazioni e dispositivi crittografici. Sono supportate le seguenti modalità di interfacciamento:
  - Microsoft CryptoAPI (Internet Explorer, Outlook, MS GINA dll);
  - PKCS#11;
  - ACOMX/BSI XSI (utilizzato dai prodotti ActivIdentity).

Si osservi che il sistema non prevede alcuna interazione diretta fra la componente ActivClient ed i moduli lato server.

## **2.9. CONSOLE DI AMMINISTRAZIONE**

Poiché il CMS è completamente web-based, esso può essere amministrato da qualsiasi workstation tramite browser. L'accesso alle funzionalità di amministrazione è consentito solo agli utenti in possesso delle opportune credenziali (certificati digitali rilasciati dalla certification authority).

Sulle console di amministrazione dalle quali devono essere svolte operazioni che richiedono l'accesso ai dispositivi crittografici (esempio: emissione di smart card o USB key) deve essere installato ActivIdentity ActivClient.

Data documento: 8 Novembre 2006	Autore: Marco Bettini	Revisore: Valeriano Bedeschi	Codice documento: OFF-20061106.mb42	Pagina: 7 di 8
------------------------------------	--------------------------	---------------------------------	--	-------------------

<b>Titolo documento:</b>	<b>Tipo documento:</b>	<b>Versione:</b>
Offerta per Sipra S.p.A. 20061106.mb42	Offerta	1.0

### **3. QUOTAZIONE PRODOTTI ACTIVIDENTITY**

Pos	Descrizione Prodotto	Costo Unitario	Q.tà	Costo scontato per quantità	Costo totale
1	Actividentity Smart Card 64K v2 - No Profile	€ 19,00	200	€ 17,00	€ 3.400,00
1	EAC Solution (CMS + AC PKI Only) for Windows including Actividentity Smart Card 64K v2 - No Profile	€ 91,75	600	€ 59,75	€ 35.850,00
1	Maintenance for EAC Solution (CMS + AC PKI Only) for Windows	€ 18,35	600	€ 11,95	€ 7.170,00
<b>TOTALE A VOI RISERVATO</b>					<b>€ 46.420,00</b>

Hacking Team è disponibile ad emettere offerta anche per i servizi professionali di progettazione, disegno architettuale, installazione, configurazione e messa in esercizio della soluzione.

### **4. CONDIZIONI GENERALI**

Tutti i prezzi esposti nella presente offerta sono da intendersi IVA esclusa.

Validità offerta:	30 gg dalla data della presente per un ordine dariceversi entro il 31/12/2006
Fatturazione prodotti:	alla consegna
Liquidazione fatture	60 D.F.F.M.
Trasporti	Ns. carico
Garanzia	A norma di legge

Data documento: 8 Novembre 2006	Autore: Marco Bettini	Revisore: Valeriano Bedeschi	Codice documento: OFF-20061106.mb42	Pagina: 8 di 8
------------------------------------	--------------------------	---------------------------------	--	-------------------