TEL VOX
SECURITY & CONSULTING

www.telvox.com

MBM

Multifunction Buffer Manager

Framework/API multipiattaforma per lo sviluppo di applicazioni di sicurezza

Multifunction Buffer Manager MBM

Il prodotto MBM è si articola in **27 applicazioni**. Ognuna di esse permette di gestire mediante un unico comando operazioni complesse.

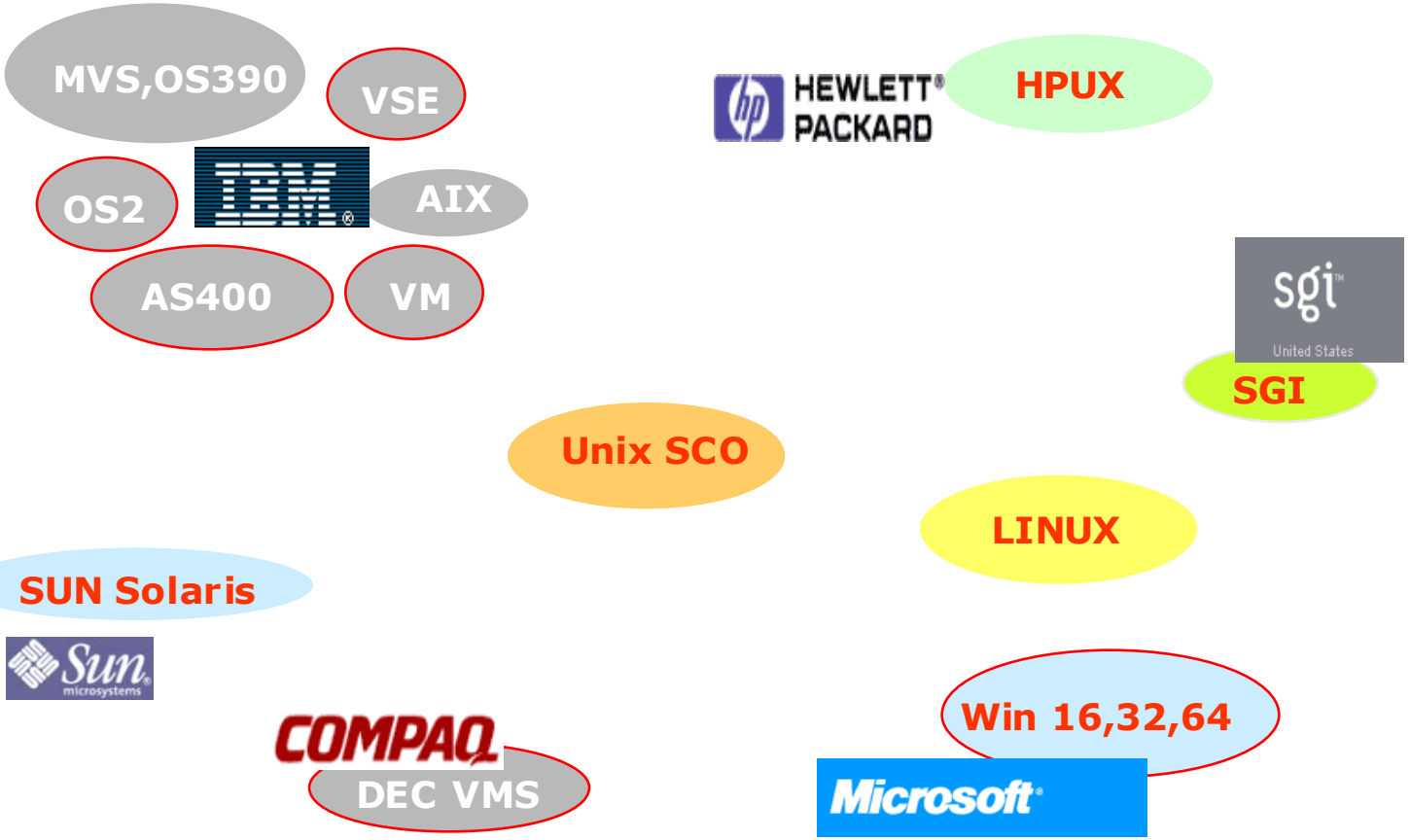
Le 27 applicazioni sono disponibili sia in formato oggetto che eseguibile e prevedono il trattamento di files in input e l'esito delle elaborazioni su file di output. Al termine delle elaborazioni eseguite viene restituito un return code che indica l'esito delle operazioni ed opzionalmente la scrittura di un file di log.

Il framework MBM è scritto integralmente in "C" secondo lo standard ANSI ed è attualmente disponibile sulle più importanti piattaforme del mercato.

Funzioni

- **Compressione e trasformazione alfabeti**
- **Hashing e crittografia simmetrica**
- **Crittografia asimmetrica e firma digitale in formato PKCS#7**
- **Gestione chiavi in formato PKCS#1-5-8-12**
- **Gestione richieste di certificato, certificati e CRL in formato X509**
- **Gestione Time Stamping in formato RFC3161**
- **Analisi di strutture asn.1**

Piattaforme



Applicazioni

- **CODA** (Compressione dati e conversione formato fisico dei file)

Gestione di una libreria in cui vengono compressi i file dei quali ne vengono conservate le caratteristiche fisiche per le opportune trasformazioni tra sistemi operativi differenti. Di ogni file viene garantita l'integrità dei dati.

- **TA** (Trasformazione alfabeti)

Trasformazione dell'alfabeto di un file in input e scrittura delle elaborazioni eseguite su un file in output.

- **HASH** (Hashing)

Calcolo dell'hash di un file e scrittura delle elaborazioni eseguite su un file in output.

Applicazioni

- **CSYM** (Crittografia simmetrica)

Criptazione/decriptazione in modo simmetrico di un file e scrittura delle elaborazioni eseguite su un file in output.

- **CASYM** (Firma e verifica flesso dati – iso 11166)

Firma , autenticazione o stampa informazioni del flusso dati in formato Iso 11166-2.

- **ASN1** (Analizzatore asn.1)

Verifica e stampa il contenuto di una struttura dati asn.1, rappresentata in formato ber o der, letta da un file in input. Opzionalmente scrive l'esito delle elaborazioni eseguite su un file in output.

- **DB** (Data base a chiavi)

Gestione di un archivio mediante indici.

Applicazioni

- **X509RSA** (Gestione chiave rsa – pkcs#1)

Genera le componenti pubblica e privata di una chiave RSA con lunghezza compresa tra 256 bit e 16.384 bit, attenendosi al modello Iso 11166-2 e PKCS # 1.

- **X509REQ** (Gestione richiesta di certificato – pkcs#10)

Genera la richiesta di certificato a partire dalle componenti pubblica e privata di una chiave RSA.

- **X509CRT** (Gestione certificato – itu x509 v3)

Genera un certificato in formato X509 v3. Tale operazione viene realizzata mediante la firma della richiesta di certificato con la componente privata della chiave RSA dell'entità di certificazione.

- **X509CRL** (Gestione lista certificati revocati – itu x509 v2)

Genera una CRL in formato X509 v2. La CRL viene firmata dall'entità di certificazione mediante la componente privata della chiave RSA.

Applicazioni

MBM

- **PADFILE** (Padding/depadding del file)

Padding/depadding di un file per consentire la gestione dell' input/output a blocchi di lunghezza fissa.

- **ISO9796** (Firma e verifica flusso dati pkcs#7 – data)

Firma , autenticazione o stampa informazioni del flusso dati in formato Iso 9796-2.

- **P7DATA** (Imbustamento flusso dati in formato pkcs#7 – data)

Imbustamento, disimbustamento, verifica e stampa informazioni del flusso dati in formato Pkcs #7 ver. 1.5.

- **P7DIGST** (Imbustamento flusso dati in formato pkcs#7 – digested)

Tra i modelli di imbustamento dati previsti nel documento Pkcs #7 ver. 1.5, gestisce solo il tipo digested data

Applicazioni

MBM

- **P7ENCRY** (Imbustamento flusso dati in formato pkcs#7 – encrypted data)

Imbustamento, disimbustamento, verifica e stampa informazioni del flusso dati in formato Pkcs #7 ver. 1.5.

- **P7ENVLP** (Imbustamento flusso dati in formato pkcs#7 - enveloped data)

Imbustamento, disimbustamento, verifica e stampa informazioni del flusso dati in formato Pkcs #7 ver. 1.5. Il modello implementato è di tipo *enveloped data* (dati con indicazione di uno o più destinatari).

- **P7SIGND** (Imbustamento flusso dati in formato pkcs#7 – signed data)

L'applicazione gestisce, tra i modelli di imbustamento dati previsti nel documento PKCS # 7 ver. 1.5, solo il tipo "signed data" (dati firmati da uno o più mittenti).

Applicazioni

- **P7SIENV** (Imbustamento flusso dati in formato pkcs#7 – signed and enveloped data)

Trasformazione, disimbustamento, verifica e stampa informazioni del flusso dati in formato Pkcs #7 ver. 1.5. Il modello è di tipo signed and enveloped data (dati criptati e firmati con indicazione del mittente o dei mittenti e del destinatario o dei destinatari).

- **PKCS8** (Gestione chiave rsa – pkcs#8)

Conversione, verifica, nuova criptazione e stampa della chiave rsa in formato Pkcs #8. la chiave rsa deve essere stata generata mediante l'applicazione X509RSA.

- **P12BAG** (Gestione chiave safeBag – pkcs#12)

Incapsulamento, disincapsulamento, verifica e stampa di una SafeBag in un SafeContents. L'applicazione permette di trattare i seguenti sei tipi di dati: chiave rsa in formato Pkcs #8 non criptato, chiave rsa in formato Pkcs #8 in formato criptato, certificato in formato X509v3 o SDSI, crl in formato X509v2.

Applicazioni

- **P12SAFE** (Gestione AuthenticatedSafe – pkcs#12)

Incapsulamento, disincapsulamento, verifica e stampa di un SafeContents in un AuthenticatedSafe. Il SafeContents viene trasformato in una busta Pkcs #7 ed inserito in un AuthenticatedSafe.

- **P12PFX** (Gestione pfx – pkcs#12)

Inclusione in una busta Pkcs #7 (data o signed data), contenente un AuthenticatedSafe, di un PFX-Protocol Data Unit. È possibile, in modo opzionale, attivare un servizio di protezione dell'integrità fisica dei dati realizzato mediante l'algoritmo Hmac-Sha1.

- **SCM** (Smart Card Manager)

Applicativo che permette di gestire i supporti (Smart Card, Smart Card Reader, Floppy Disk, …) su cui vengono generalmente archiviate le chiavi ed i relativi certificati.

Applicazioni

- **TSAREQ** (Gestione di una time stamp request)

Imbustamento, disimbustamento, verifica e stampa di una time stamp request.

- **TSATOK** (Gestione di una time stamp token)

Imbustamento, disimbustamento, verifica e stampa di un time stamp token.

- **TSARES** (Gestione di una time stamp request)

Imbustamento, disimbustamento, verifica e stampa di una time stamp response.

Principali Referenze

MBM

CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

Dipartimento del Tesoro
Ministero dell'Economia e delle Finanze MEF

INPS
Istituto Nazionale Previdenza Sociale

Getronics
ICT SOLUTIONS AND SERVICES

TORO ASSICURAZIONI

MEF Ministero dell'Economia e delle Finanze

FIAT

Finsiel

seceti

A22 Autostrada del Brennero s.p.a.
Brennerautobahn AG