L’e-Government dell’ateneo Federico II

CSI- Area Tecnica e-Government

Clelia Baldo

La firma digitale

La firma digitale - Generalità

- La firma digitale è basata su un procedimento di “crittografia asimmetrica” che fa uso di una coppia di chiavi: una privata (utilizzata per firmare) ed una pubblica (utilizzata per le operazioni di verifica della firma).
- La corrispondenza tra le chiavi di firma ed il sottoscrittore è garantita da una terza parte fidata, il certificatore qualificato.
- Il certificatore (qualificato) genera e consegna a ciascun titolare un dispositivo sicuro di firma contenente: la coppia di chiavi assieme ad un certificato qualificato di firma che consente l’associazione della persona con la sua chiave pubblica.
- Il certificatore (qualificato) gestisce l’identificazione e la registrazione certa del richiedente, nonchè la sospensione temporanea della validità o la revoca definitiva del certificato qualificato.

Il Codice dell'amministrazione digitale e la firma digitale

- Il documento informatico sottoscritto con **firma digitale**
  - ✓ soddisfa il requisito legale della forma scritta,
  - ✓ ha efficacia giuridico-probatoria.

- La firma digitale garantisce autenticazione, non ripudio (fino a querela di falso da parte del sottoscrittore) e l'integrità del documento informatico sottoscritto.

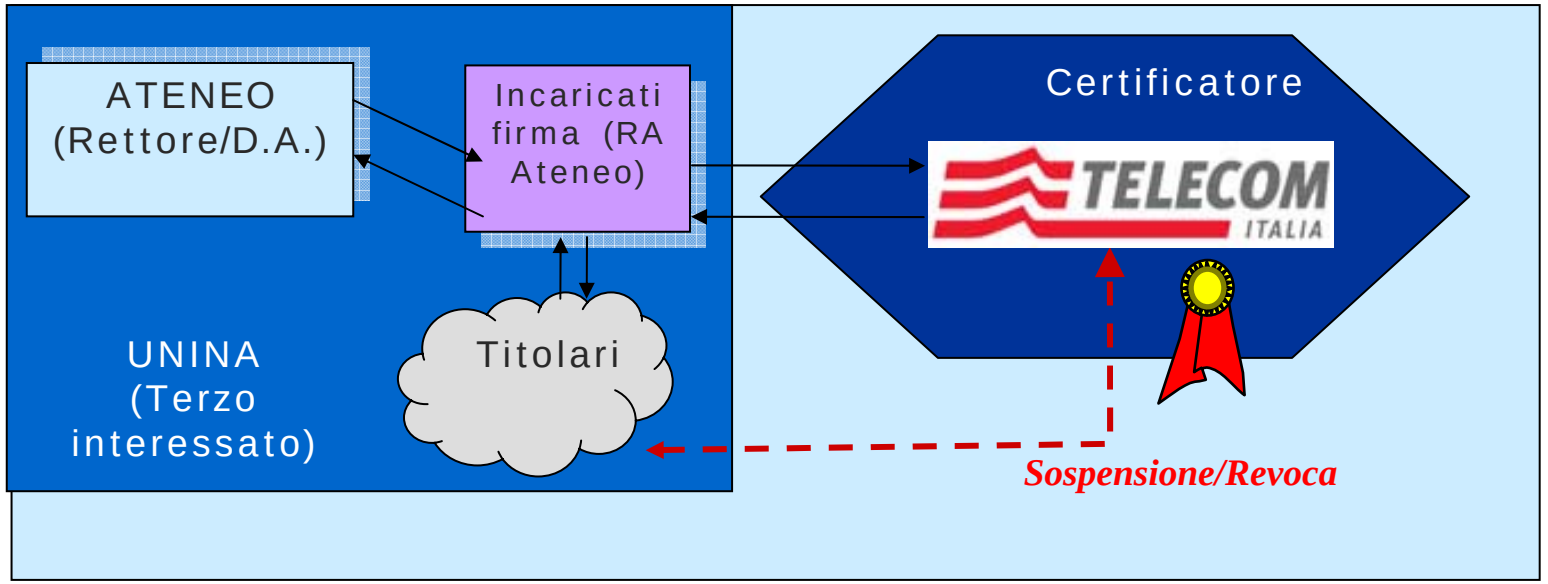
- L'uso della firma digitale integra e sostituisce ad ogni fine di legge l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi comunque previsti.

Il servizio firma digitale dell'Ateneo (1/2)

- L'Ateneo, in qualità di "terzo interessato", si avvale dei servizi offerti dal **certificatore accreditato** **IT Telecom S.r.l..**
- Il servizio si basa sulla organizzazione di una "Registration Authority" interna, costituita da amministrativi dell'Ateneo all'uopo incaricati dalla Direzione Amministrativa, delegati dal Certificatore.
- I dispositivi sicuri di firma, contenenti la chiave crittografica di sottoscrizione ed il certificato del titolare, sono costituiti da "**token USB**".
- I certificati qualificati sono assegnati ai responsabili di struttura o ad altri soggetti, secondo le indicazioni fornite dal Rettore e dal Direttore Amministrativo.
- La firma digitale, integrata nell'architettura funzionale e di servizio del sistema di e-Government Praxis, può essere utilizzata, in particolare, per il Protocollo Informatico e l'e-Procurement.

Il servizio firma digitale dell'Ateneo (2/2)

- **E' stato emanato il Regolamento di Ateneo in materia di Posta Elettronica Certificata, con la definizione di:**
  - ✓ **Regole per l'assegnazione, la sospensione e la revoca dei certificati da parte dell'Ateneo,**
  - ✓ **Compiti e responsabilità dell'Ateneo (nella figura della propria «Registration Authority» interna) nei confronti del Certificatore, e dei Titolari di certificato qualificato,**
  - ✓ **Diritti dell'Ateneo, in qualità di "terzo interessato" ed adempimenti dei Titolari.**



Il processo di apposizione della firma digitale

CSI – Area tecnica e-Government

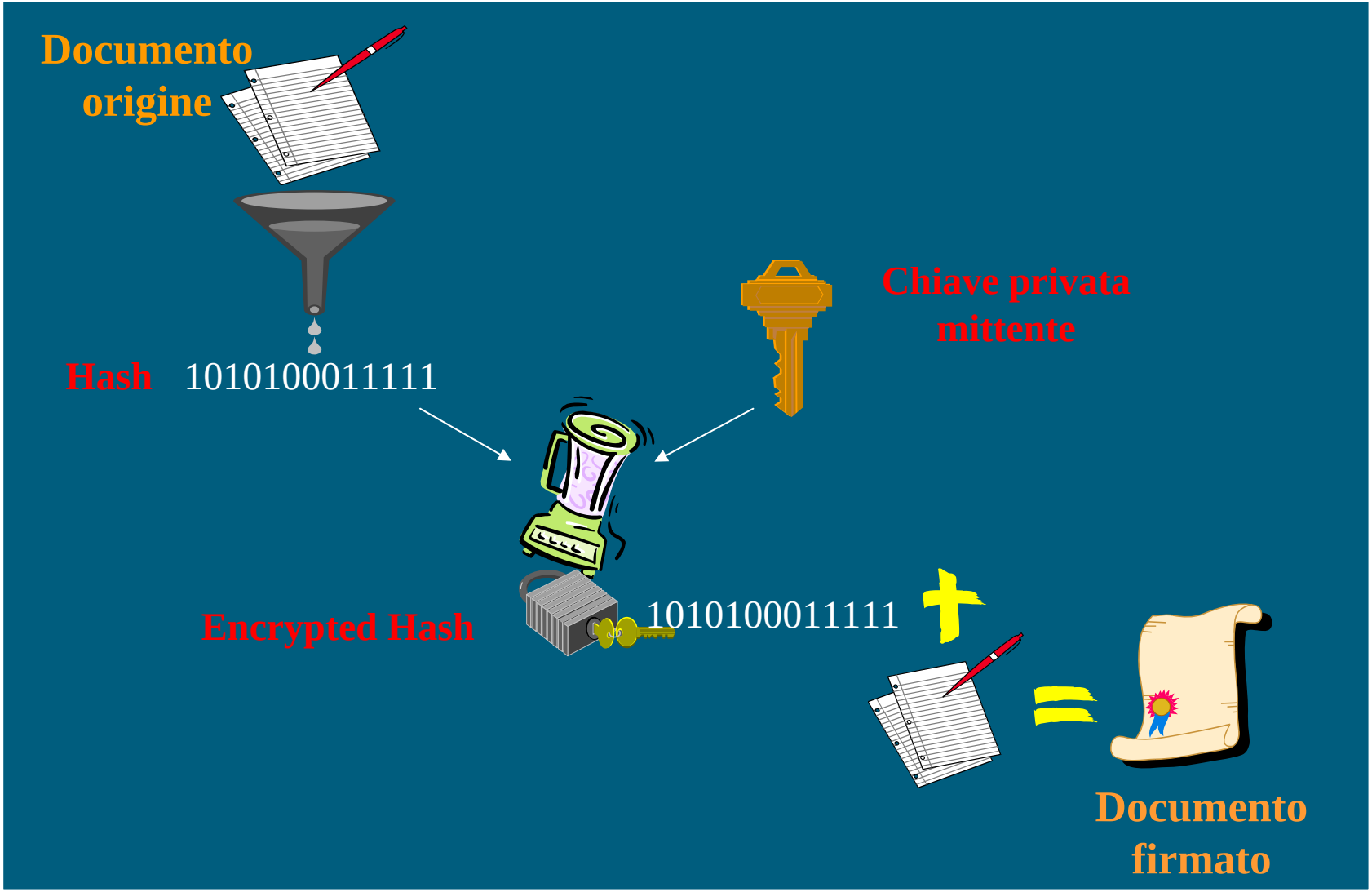
Calcolare il valore dell'impronta del documento

Cifrare il valore dell'impronta calcolata utilizzando la chiave privata del sottoscrittore

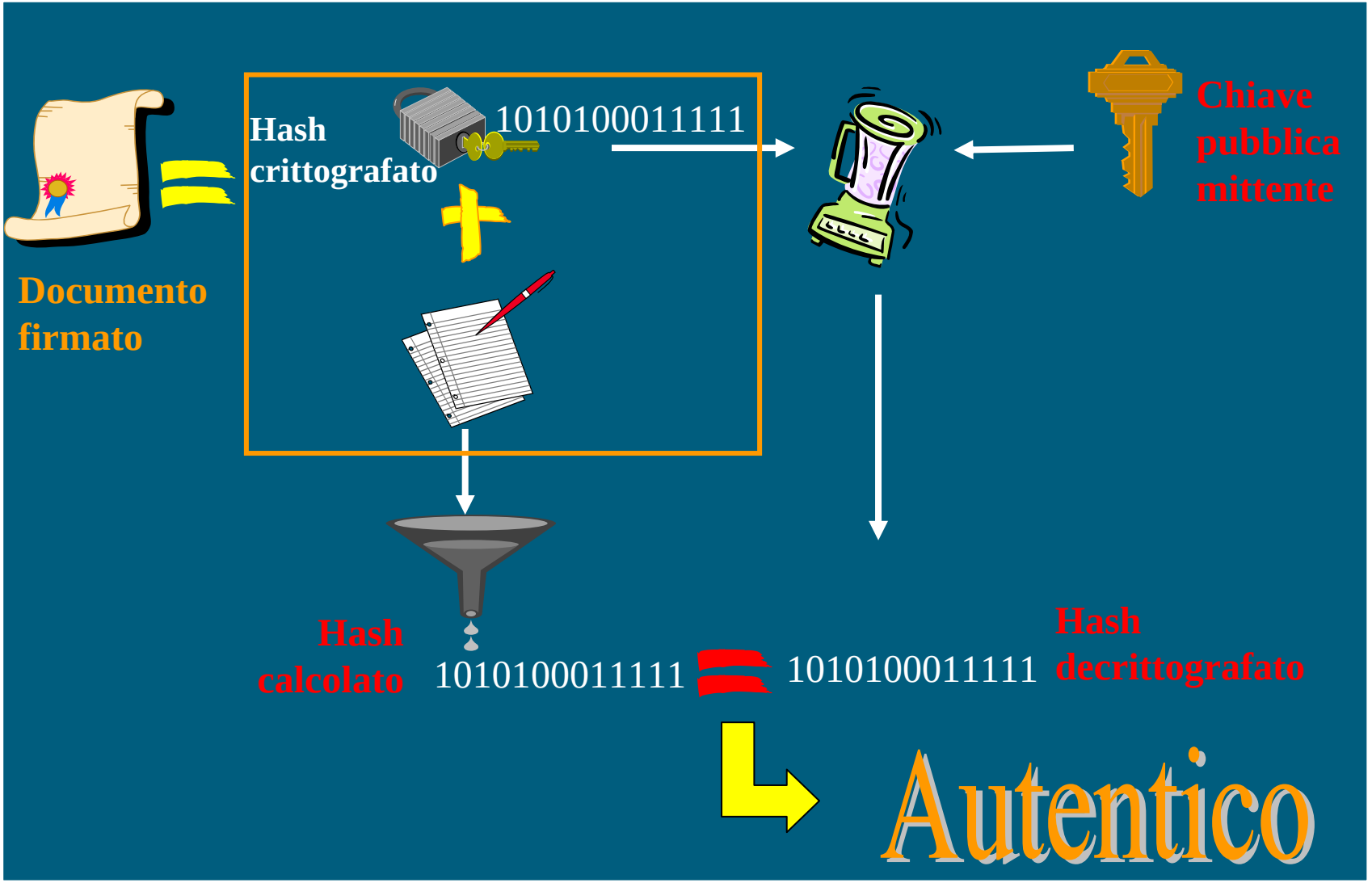
Aggiungere al documento originale la firma digitale ed il certificato qualificato del sottoscrittore

DOCUMENTO INFORMATICO FIRMATO

Il processo di firma



La verifica della firma digitale

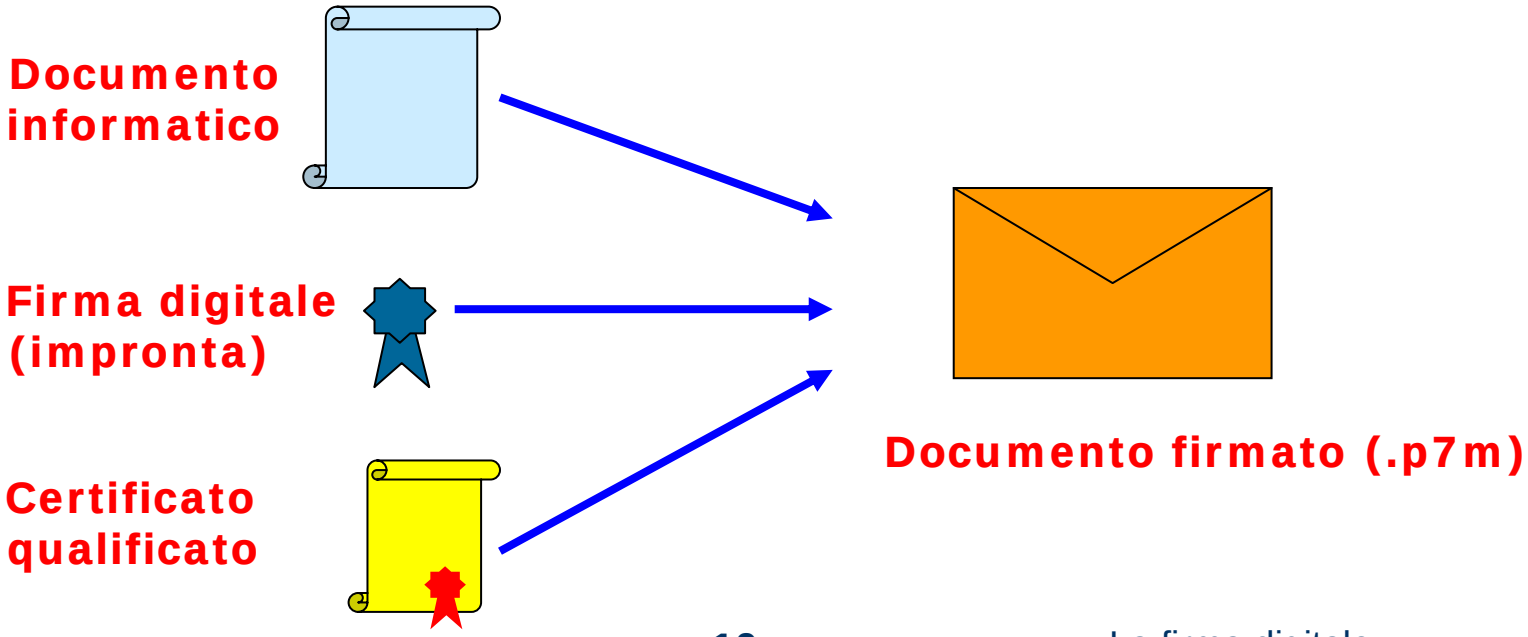


Il certificato qualificato

- Il certificato di firma è un documento elettronico che, oltre a contenere i dati essenziali del titolare, ne contiene la chiave pubblica:

Il formato di firma

- Il documento da firmare è imbustato nel formato originale, senza aggiunte in testa o in coda al formato stesso. Il file firmato, ossia la busta, contiene al suo interno:
  - **il documento informatico nel formato originale,**
  - **la firma digitale ad esso associata (l'impronta),**
  - **il certificato qualificato del sottoscrittore.**



Come apporre e verificare la firma digitale

- Il titolare deve apporre in chiaro, nel documento, il proprio ruolo, il nome, il cognome e la data di sottoscrizione.
- Il titolare deve trasformare il documento informatico in formato pdf, eventualmente adoperando strumenti di tipo "open source", scaricabili anche dal sito http://www.praxis.unina.it.
- Per firmare il documento, è sufficiente eseguire l'applicazione DigitalSign, il cui CD di installazione è contenuto nel kit di firma.
- Il file ".p7m" ottenuto può quindi essere conservato su supporto magnetico, oppure trasmesso mediante strumenti telematici (Posta Elettronica o Posta Elettronica Certificata).
- La verifica di autenticità e di integrità del file firmato può essere eseguita con un qualunque strumento di verifica, tra cui il prodotto DigitalSign reader che può essere scaricato dal sito http://www.praxis.unina.it.

Alcune informazioni operative

- **E' consultabile il calendario, predisposto dagli *Incaricati_firma* dell'Ateneo, degli incontri per l'identificazione dei titolari.**
- **Ciascun interessato è pregato di confermare con gli *Incaricati_firma* la data e l'ora dell'incontro, inviando una e-mail all'indirizzo:**

  firma.digitale@unina.it

- **Per velocizzare la procedura di identificazione, è opportuno che ciascun interessato precompili i moduli di adesione, disponibili sul sito:**

  http://www.praxis.unina.it

- **Le istruzioni per l'utilizzo e la custodia del dispositivo sicuro di firma sono contenuti nel "Manuale d'uso del servizio di firma digitale".**


SISTEMA
PRAXIS
UNINA
E-GOVERNMENT
UNIVERSITA' DEGLI STUDI DI NAPOLI FEDERICO II
HOME
NORMATIVA
E-GOVERNMENT
PROTOCOLLO
FIRMA DIGITALE
PEC
SERVIZI
DOWNLOAD
SERVIZI
PRAXIS
e-government
PEC
Firma Digitale
Protocollo informatico
NEWS
»6 febbraio 2007
L'e-government in Federico II
Il Rettore interverrà alla presentazione organizzata dal C.S.I. per illustrare il piano di e-government del nostro ateneo e le iniziative in corso. L'evento si svolgerà il 6 febbraio presso la sala rossa del complesso di Monte S. Angelo, alle ore 12. [Leggi tutto]
»1 gennaio 2007
A decorrere dal 1 gennaio 2007, a seguito alla positiva conclusione della fase di sperimentazione del Progetto Protocollo Informatico, è istituito il "Protocollo Generale dell'Università degli Studi di Napoli Federico II" e viene avviato l'esercizio del "Sistema di protocollo informatico" che, in accordo con la normativa vigente in materia, consente anche la gestione informatica dei documenti e dei procedimenti amministrativi. Al Sistema sono inizialmente collegate le seguenti strutture: l'Amministrazione Centrale, i Poli, il Dipartimento di Informatica e Sistemistica, il Dipartimento di Scienze Fisiche ed il Centro Servizi Informativi di Ateneo (CSI). Le Facoltà ed i restanti Dipartimenti e Centri dotati di autonomia amministrativo contabile adotteranno progressivamente il Sistema di
LINKS UTILI
CNIPA
PROTOCOLLO GOV
INNOVAZIONE PA GOV
POSTECOM
FIRMASICURA