

# IANUS Authentication Station

*Sicurezza dei Sistemi Informativi*

## 1. L'AUTENTICAZIONE DEGLI UTENTI

L'**autenticazione** di un utente è il processo attraverso il quale la sua identità viene verificata. L'adeguata protezione di un sistema informativo si basa generalmente sull'adozione di tre fattori.

Il primo avviene tramite digitazione di una password segreta. Tale metodo è il più comune ma sicuramente anche il più vulnerabile.

La seconda soluzione implica l'attribuzione ad un utente del diritto di accedere a delle risorse sulla base di una sua propria caratteristica fisica come, ad esempio, l'impronta digitale o il timbro della voce. Questo tipo di autenticazione è molto sicuro ma poco diffuso a causa degli alti costi.

L'ultimo tipo implica il fatto che un utente possieda un dispositivo che risulti tecnicamente molto difficile da replicare.

Come tutti i componenti di base della tecnologia Ianus, **Ianus Authentication Station** possiede tale caratteristica ed è il sistema di autenticazione sviluppato da Cineca per venire incontro alle problematiche di sicurezza legate ai sistemi legacy.

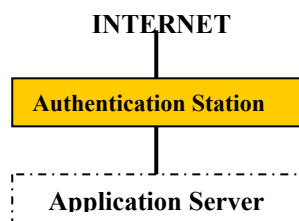


Figura 1 - Architettura

## 2. IANUS AUTHENTICATION STATION

Lo scopo principale della **Ianus Authentication Station** è quello di consentire il controllo degli accessi a sistemi informativi che non adottano forti politiche di sicurezza.

È composta da:

- **Server Ianus**: server di derivazione dal server Apache. È integrato con estensioni SSL e per il dialogo con il Monitor. Qualora il client lo permetta, è in grado di negoziare un canale crittografato con crittografia forte. Allo stato attuale RC4 128 BIT e 3DES 168 BIT. L'uso di componenti Open Source di larghissima diffusione permette di mantenerlo aggiornato.

- **Monitor**: modulo di autenticazione e controllo dell'accesso alle risorse del server Ianus. Verifica

le richieste del client sulla base di regole definite in un database per l'amministrazione del servizio. Può validare l'utente secondo i normali standard web (username e password) oppure, dialogando con la sua contropartita lato client, lo IanusGate, permettere l'accesso alle risorse solo agli utenti accreditati. La flessibilità del prodotto consente di impostare livelli di accesso (pubblico, con sola password o mediante IanusGate)

- **Amministrazione**: strumento che, attraverso un'interfaccia web, permette la gestione dell'accessibilità alle risorse di utenti, funzioni, gruppi di funzioni e di utenti.

- **IanusGate lato-client**: software client da installarsi sulle macchine da abilitare all'accesso ai servizi. È il corrispettivo lato client dello Server Ianus nonché il suo naturale complemento in quanto, attraverso un protocollo ad hoc, è in grado di dialogare con esso.

Tra le caratteristiche più importanti:

- capacità di negoziare un canale crittografato con il più alto livello di crittografia attualmente disponibile

- radicamento, ovvero non può essere duplicato in un'altra postazione di lavoro

- periodica negoziazione con il server del cambio di credenziali in maniera trasparente e indipendente dall'utente.

## 3. STRUTTURA DEL FLUSSO INFORMATIVO

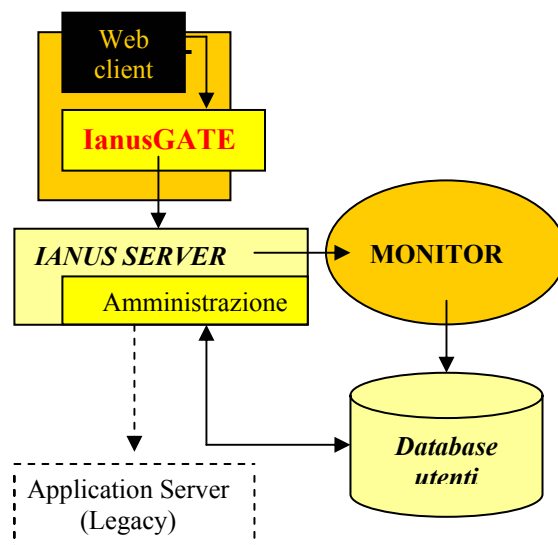


Figura 2 - Flusso Informativo

In pratica, la **Ianus Authentication Station** viene posta tra il sistema informativo al quale l'utente (client) desidera accedere e l'applicazione target stessa.

Attraverso lo IanusGate le richieste del client vengono filtrate, e, se validate, trasmesse all'applicazione server.

Se invece l'utente non risulta abilitato ad accedere alle risorse, il risultato della richiesta sarà una pagina che indica il mancato permesso.

La seguente Figura 3 illustra il percorso della richiesta proprio nel caso in cui l'utente non possieda l'abilitazione:

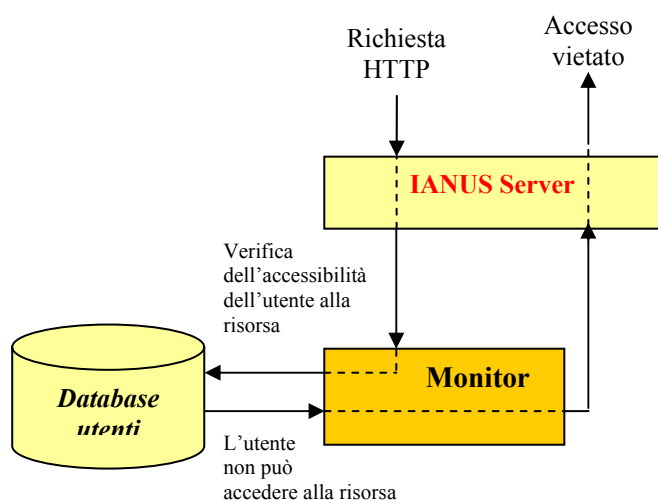


Figura 3 - Accesso non abilitato

#### 4. PERCHÉ IANUS AUTHENTICATION STATION

I vantaggi che derivano dall'uso di **Ianus Authentication Station** sono molti:

- l'unione Server Ianus/IanusGate permette di attuare un sistema di autenticazione più sicuro rispetto al metodo di autenticazione basato su username e password dei tradizionali clients/servers http.
- controllo dell'utenza senza la necessità di implementare complessi meccanismi di sicurezza
- facile gestione delle utenze (creazione, modifica e revoca dei permessi) tramite un interfaccia web da remoto rappresentata in Figura 4

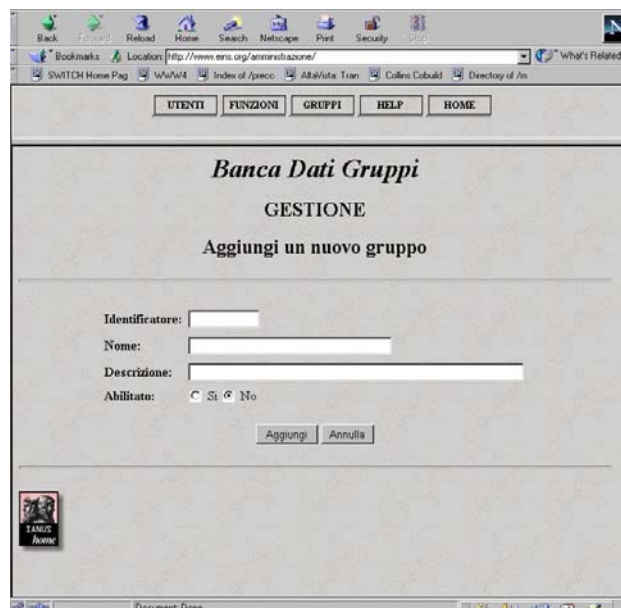


Figura 4 - Interfaccia web per la gestione utenze

- il fatto che il software IanusGate abbia la caratteristica di radicarsi garantisce che le operazioni svolte da un determinato IanusGate possano avere luogo solo attraverso una macchina nota e identificabile.