CIFRATURA MASSIVA PASSWORD

In questo documento sono riportati tutti gli aspetti da tener presente in caso di cifratura di tutte le password utente su Esse3.

ALGORITMI DI CIFRATURA SUPPORTATI

ID	ENCRYPTION_TYPE
1	*UNIXCRYPT* *
2	*MD4*
3	*MD5* *
4	*SHA-1* *
5	*MD5-BASED* *
6	*SHA-1/B64* *
7	*MD4/B64*
8	*MD5/B64* *
9	*RSA-BASED*
10	*RSA-BASED/B64*
11	*SHA-1/U8* *
12	BCRYPT *
13	*SHA-256*
14	*SHA-512* *
15	SSHA *

***= algoritmi consigliati**

CONTROLLI PREVENTIVI

Prima di procedere con la cifratura delle password è necessario considerare l'impatto della modifica anche con eventuali integrazioni di ESSE3 con sistemi esterni.

ESISTE INTEGRAZIONE ESTERNA

Nel caso in cui, sia prevista una integrazione con LDAP/AD (in House o Hosting Cineca) alimentato con le credenziali utenti di Esse3, è necessario modificare l'architettura dell'integrazione stessa in modo da poter supportare lo scambio del dato tra i sistemi con la cifratura delle password, effettuando le modifiche necessarie alle procedure di integrazione per recepire la direttiva "cifrata" per lo scambio password.

- **SE il provisioning avviene mediante procedure standard di Esse3** (Servizi di Replica), oltre a quando definito nel paragrafo COME AVVIENE LA CIFRATURA?, sarà necessario una modifica alla configurazione in essere, a carico dei consulenti Cineca. E' inoltre necessario valutare che l'algoritmo scelto sia conforme con quello utilizzato in LDAP/AD.

- **SE il provisioning è eseguito da procedure esterne a Esse3** e gestite tramite sistemi dell'ateneo, dopo aver attivato il parametro per definire l'algoritmo di cifratura non sarà più possibile accedere ai dati delle password "in chiaro" e, di conseguenze, occorrerà valutare un adeguamento alle proprie procedure o allinearsi alle procedure standard di Esse3 (Servizi di replica).

NON ESISTE INTEGRAZIONE ESTERNA

Nel caso in cui non vi siano integrazioni o che non vi siano impatti sulle integrazioni in essere, in questo caso, l'autenticazione sarà certamente in Esse3 (e tutte le password sono memorizzate sul db di Esse3): si può procedere seguendo le istruzioni riportate nel paragrafo COME AVVIENE LA CIFRATURA?.

AUTENTICAZIONE TRAMITE IDP (SHIBBOLETH)

in questo caso occorre conoscere la logica di autenticazione dell'IDP che potrebbe autenticare su un LDAP (per alcuni gruppi utente) e su ESSE3 (in "*fallback*", per altri):

- Nel primo caso, vale quanto detto nel paragrafo ESISTE INTEGRAZIONE ESTERNA.
- Nel secondo caso, vale quanto detto nel paragrafo NON ESISTE INTEGRAZIONE ESTERNA , ma sarà necessario allineare (e comunicare al gestore dell'IDP) l'algoritmo di cifratura utilizzato. Nel caso IDP sia gestito da Cineca, sarà cura dei consulenti Cineca configurare IDP di conseguenza.

Nota: Occorre tenere presente, in caso di integrazione di ESSE3 con SSO (IDP) Cineca, che il connettore supporta i seguenti algoritmi di cifratura:

- WLS
- SHA
- SSHA
- MD5
- MD5BASE64
- UNIXCRYPT
- APACHECRYPT
- IANUSCRYPT
- CLEARTEXT

Di conseguenza è indispesanbile che la scelta dell'algoritmo di cifratura passowrd lato ESSE3 ricada sull'analogo impostato lato SSO/IDP di CINECA

Ovviamente, in questo caso, se l'IDP autentica su un LDAP occorre fare le stesse valutazioni relative al provisioning dello stesso: se sono eseguite da servizi di replica Esse3 o se tramite altra modaltà esterna ad Esse3.

COME AVVIENE LA CIFRATURA?

La cifratura delle password avviene definendo innanzitutto l'algoritmo tra quelli supportati da Esse3. La lista degli algoritmi è presente nella tabella

P18_PWD_CRYPT

Dopo aver individuato l'algoritmo che si preferisce adottare (vedi algoritmi supportati) sarà necessario valorizzare il parametro di configurazione (par_conf) **PWD_ENCRYPTION** (Prodotto: ESSE3 - Modulo: FRK) con l'ID dell'algoritmo scelto.

Il VAL_NUM del parametro deve essere valorizzato con l' ID della tabella P18_PWD_CRYPT dell'algorimto scelto.

Dal momento in cui viene configurato il parametro, tutte le variazioni/creazioni delle password di tutti gli utenti (appartenenti a qualsiasi gruppo) subiranno la cifratura e il campo password (P18_USER.USER_PWD) non sarà più in chiaro.

L'algoritmo di cifratura scelto, sarà uguale per tutti gli utenti e non è possibile differenziarlo per gruppi di utenti.

Come cifrare le password preesistenti?

Dopo aver valorizzato il parametro per cifrare le password, sarà necessario procedere alla cifratura di tutte le password create prima di questa configurazione.

Nella maschera CIFRATURA DELLE PASSWORD UTENTI (nel menu Gestione sicurezza Funzioni/Entità/Gruppi/Utenti) vi è un solo ed unico pulsante per cifrare tutte le password di tutti gli utenti. **L'azione sul pulsante è irreversibile**.

NOTA: se per l'ateneo è previsto un servizio di provisioning verso LDAP (o Active Directory) tramite il servizio di REPLICHE, la cifratura massiva farebbe scattare una replica per ogni utente per cui si fa la cifratura (quindi tutti i record degli utenti nella P18_USER).

Si consiglia fortemente di disattivare le repliche per il tempo necessario al processo di cifratura massiva per evitare di accodare migliaia di repliche e appesantire l'intero database. Per disattivare le repliche è sufficiente disabilitare il parametro di configurazione EPI_REPLICA_DATI (=0). Successivamente, andrà riabilitato il parametro (=1).