

Toro Assicurazioni

Progetto di Strong Authentication e SSO per le transazioni CICS critiche e dispositive

Studio di fattibilità

Obiettivo

Con lo scopo di aumentare il livello di sicurezza, il Gruppo Toro Assicurazioni intende implementare un sistema che permetta l'adozione di uno strumento di Strong Authentication in merito alle transazioni effettuate da un'applicazione di tipo legacy che risiede su piattaforma Host (ambiente CICS) e che è sviluppata in Cobol. Secondo il Gruppo Toro si rende necessario questo intervento in considerazione dell'importanza che ricopre l'applicazione che tratta il Ramo Vita all'interno del business aziendale. Si intende quindi attivare un secondo livello di autenticazione che garantisca l'effettiva identità dell'utente che in quel momento effettua l'operazione.

Specifica

La specifica richiesta dal Gruppo Toro, mediante capitolato tecnico, consiste nel fatto che: "ogni volta che l'utente dovrà utilizzare una determinata transazione dell'applicazione Life il sistema di autenticazione gli chiederà di inserire, in quel preciso momento, l'elemento di autenticazione forte. L'elemento richiesto non dovrà comportare pesanti modifiche all'applicazione, ma dovrà consentire una facile implementazione; inoltre dovrà potersi integrare con il sistema di autenticazione IBM Tivoli Access Manager utilizzato per le applicazioni web based (anche dall'esterno)".

La proposta dovrà anche considerare una soluzione di SSO.

]HackingTeam[

Hacking Team S.r.l.

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

Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano

e-mail: info@hackingteam.it – web: <http://www.hackingteam.it> – Fax: +39.02.63118946

Utenza

Il sistema sarà inizialmente utilizzato solo da una specifica applicazione con un numero di utenze limitato (circa 20). La soluzione proposta dovrà comunque prevedere un bacino di circa 2000 utenze.

Considerazioni

Per avvalorare e per far meglio comprendere la proposta Hacking Team in merito a quanto richiesto, si commentano di seguito alcuni punti fondamentali.

1. L'ambiente di riferimento in cui la soluzione andrà calata è estremamente eterogeneo e questo richiede all'architettura ed al prodotto utilizzati una notevole capacità/possibilità di integrazione.
2. Le informazioni a disposizione in termini tecnici non sono sufficienti a delineare una possibile soluzione funzionante a priori in maniera certa. Questo non è in nessun modo dovuto a carenze del capitolato tecnico ma ad una incapacità tecnica di rilevare le informazioni necessarie che è intrinseca nella soluzione stessa. Ovvero, senza adeguati controlli e verifiche tecniche "sul campo" non è possibile rispondere con una soluzione dettagliata sicuramente funzionante.
3. Considerando l'importanza e la criticità rivestita dall'applicativo in questione, nonché dal possibile bacino di utenza nel medio/lungo termine, è indispensabile procedere con un adeguato ed esauriente studio di fattibilità.

Proposta Hacking Team

La proposta di Hacking Team consiste in attente verifiche ed in un completo studio mirati ad ottenere quanto segue:

- verifiche tecniche di integrazione "sul campo" per ottenere tutte le informazioni necessarie all'identificazione del funzionamento ottimale,
- verifiche architetture "sul campo" per ottenere tutte le informazioni necessarie all'identificazione della soluzione ottimale,

]HackingTeam[

Hacking Team S.r.l.

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

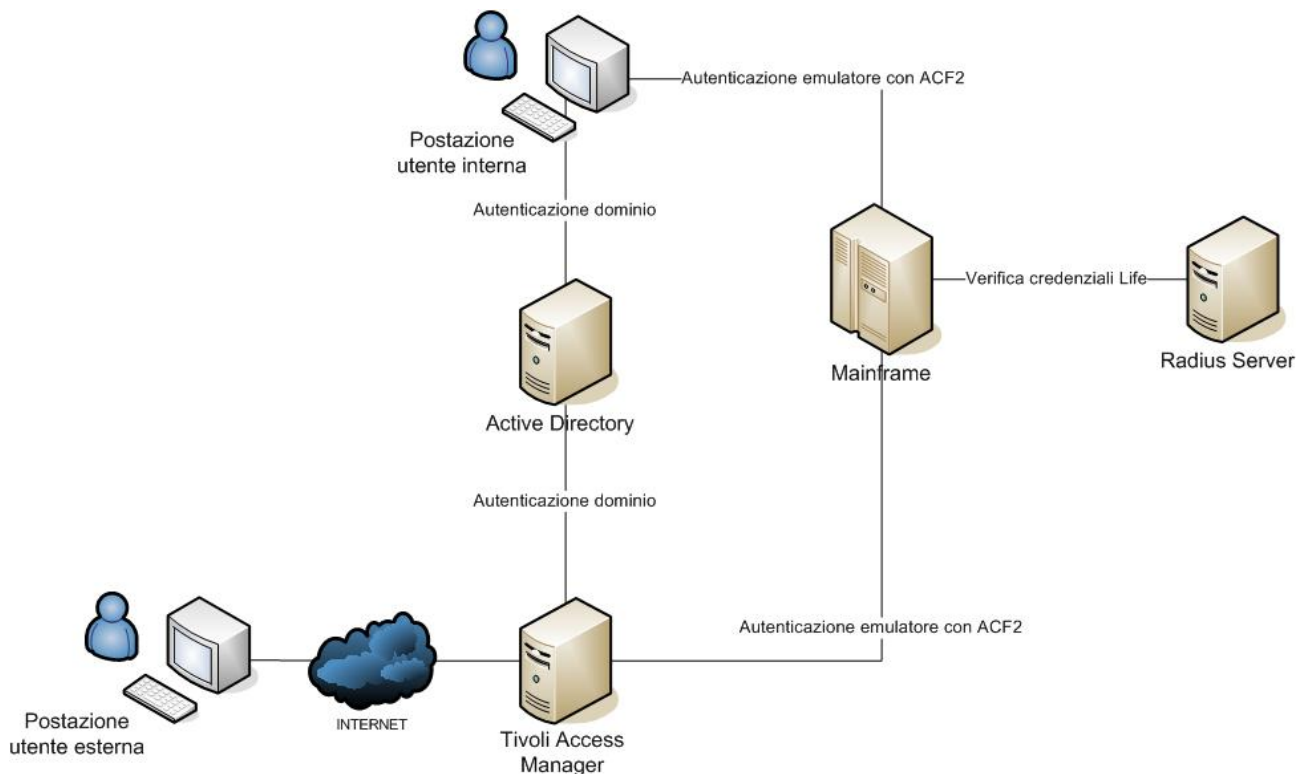
Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano

e-mail: info@hackingteam.it – web: <http://www.hackingteam.it> – Fax: +39.02.63118946

- studio di fattibilità volto ad identificare in maniera sensata e sicura una soluzione aderente ai requisiti del cliente e sicuramente funzionante,
- progettazione della soluzione che porterà alla stesura di un documento di progetto volto ad identificare le macro-fasi dell'implementazione.

In ogni caso, le strade percorribili identificate fino ad ora nelle fasi iniziali di raccolta delle informazioni sono le seguenti (entrambe contemplano sia la parte di strong authentication che la parte di SSO):

Ipotesi A: utilizzare una strong authentication implementata attraverso l'utilizzo della tecnologia OTP. Questo implica che il mainframe (ACF2), all'atto della richiesta di una "transazione Life", deve essere in grado di spedire una richiesta Radius e di saperne interpretare correttamente la risposta.



]HackingTeam[

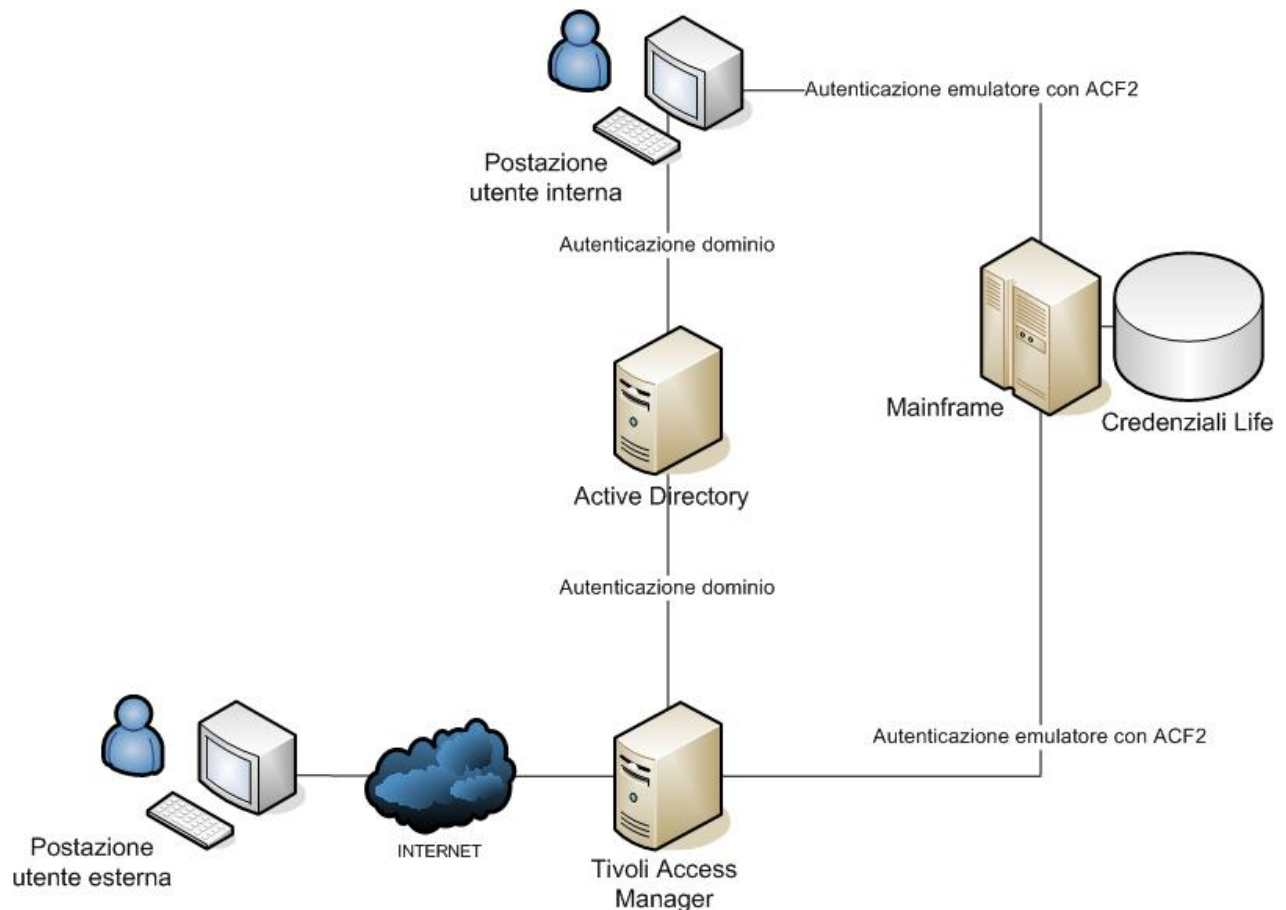
Hacking Team S.r.l.

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

Sede legale e amministrativa: Via Freguglia Carlo, 2 – 20122 Milano

e-mail: info@hackingteam.it – web: http://www.hackingteam.it – Fax: +39.02.63118946

Ipotesi B: utilizzare la tecnologia di single-sign-on attraverso una soluzione che riconosca la maschera relativa alle “transazioni Life” (operazione che abbiamo controllato essere fattibile). Questo implica che sul mainframe o in altro luogo risiedano credenziali di tipo “B”.



La scelta dell'ipotesi migliore per il Gruppo Toro Assicurazioni si potrà identificare solo a fronte di uno studio iniziale di funzionalità ed integrazioni. Tale studio è impostabile esclusivamente attraverso un opportuno pilota.