	(ossia numeri univoci usati una sola volta). Messaggi XML completamente validi possono essere usati per causare un attacco DoS chiamato "replay attack". Un attaccante può inviare messaggi SOAP ripetitivi contenenti payload XML validi e richieste ben formate replicando messaggi precedentemente osservati, per portare un attacco DoS.

Hardening dei documenti XML	
Minaccia	Negazione dei servizi (es. Coercive parsing).
Contromisure	Verificare che l'input XML sia sempre validato attraverso il corrispondente schema XML.

Hardening dei documenti XML	
Minaccia	Negazione dei servizi - Schema poisoning
Contromisure	Proteggere gli schemi XML contro modifiche non autorizzate. Un attaccante può intercettare uno schema XML prima di raggiungere un service consumer e modificarlo con uno "Schema poisoning". In tal modo, AD ESEMPIO, è possibile compromettere, lato web service, l'elaborazione dell'XML parser (che può andare in hang, crash o in uno stato inconsistente), producendo un denial of service.

5.8.3 Utenze

Ai principi generali già introdotti nel paragrafo [rif. 5.1.1], si aggiungono le seguenti indicazioni per il contesto specifico:

Utenze	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità delle informazioni. - Divulgazione di informazioni riservate.
Contromisure	Nel contesto ESB, sistemi e utenze applicative (non assegnate a persone fisiche) dovranno essere chiaramente identificati e autenticati.

5.8.4 Autenticazione

Ai principi generali già introdotti nel paragrafo [rif. 5.1.2], si aggiungono le seguenti indicazioni per il contesto specifico:

Autenticazione	
Minaccia	- Abuso di privilegi da parte dell'utente. - Accesso non autorizzato alle informazioni.
Contromisure	Lo standard SAML è una specifica di protezione basata su XML per scambiare informazioni di autenticazione e autorizzazione su un utente o un soggetto. Definisce uno XML schema e le asserzioni di sicurezza. Le asserzioni sono di tre tipi e riguardano: - l'autenticazione - gli attributi relativi alla sicurezza per il soggetto - le decisioni di autorizzazione adottate. Laddove si debbano realizzare applicazioni interoperabili (tra differenti application server) o web services richiamabili da molteplici operazioni (si pensi ad es. ad un servizio di CRM che espone i suoi metodi tramite web services ad un gran numero di altre applicazioni interne), è necessario utilizzare SAML per la gestione delle autorizzazioni applicative del soggetto che richiede i servizi in base agli attributi di sicurezza di cui dispone.