5.8.5 Autorizzazione

Ai principi generali già introdotti nel paragrafo [rif. 5.1.3], si aggiungono le seguenti indicazioni per il contesto specifico:

Autorizzazione	
Minaccia	- Accesso non autorizzato alle informazioni. - Uso non autorizzato di privilegi. - Crittografia debole o non validata. - Falsificazione di identità.
Contromisure	Si considerino i seguenti standard: - XML Signature: definisce la sintassi della firma digitale nell'ambito dei documenti XML e le regole per il suo processing. - XML Encryption: si avvale di una tecnologia a chiave condivisa. Il motivo per cui è richiesta la crittografia a livello XML (al di sopra di quella di trasporto, ad esempio SSL) è che la riservatezza dei messaggi deve essere mantenuta quando un messaggio attraversa più nodi nel suo percorso verso la destinazione. Inoltre XML Encryption conserva anche la riservatezza dei messaggi a riposo (quando cioè un messaggio XML viene memorizzato sulla destinazione finale). - XML Key Management Specification (XKMS): completa gli standard XML Signature e XML Encryption, specificando i protocolli per la distribuzione e la registrazione di chiavi pubbliche (crittografia a chiave pubblica) che possono essere utilizzate con XML Signature e XML Encryption. - WS-Security: definisce le estensioni per il protocollo SOAP per realizzare messaggistica sicura ovvero tale da garantire l'integrità, la riservatezza, l'autenticazione dei messaggi. È un meccanismo di uso generale per associare i token di sicurezza ai messaggi SOAP. Si basa su XML Signature e XML Encryption. Le funzionalità descritte, laddove richieste da un'applicazione, non devono essere implementate autonomamente partendo da zero c con librerie generiche, ma devono necessariamente utilizzare gli standard sopra elencati.

5.8.6 Crittografia

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

Utenti	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni.
Contromisure	Per la definizione delle politiche di controllo di accesso e per valutare le richieste di autorizzazione, utilizzare lo standard XACML o eXtensible Access Control Markup Language, basato su XML.

5.8.7 Documentazione

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.5].

5.8.8 Logging

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.6].