Segurança em Web Services

Introdução

Construir Web Services seguros implica em entender as ameaças em que os serviços estão expostos e ter definido qual nível de segurança deve ser alcançado. A maneira mais eficaz de se implementar segurança em aplicações é estar em consonância com os princípios, padrões e práticas. Os impactos negativos de uma falha de segurança podem comprometer os dados confidênciais, ceder acesso não autorizado e até mesmo comprometer a reputação e confiabilidade da instituição que esta prestando o serviço.
Para prover aos sistemas que utilizam a tecnologia de Web Services as seguintes recomendações são apresentadas:

Segurança no nível de aplicação:

- Prover a cifração das mensagens trocadas entre as partes utilizando *XML Encryption Syntax and Processing* e *Decryption Transform for XML Signature (XMLenc)* conforme a ***Especificação Técnica*** do ***GT 2 - Segurança*** recomenda na ***Tabela 8 – Especificações para Segurança – Desenvolvimento de Sistemas.***
- Prover a autenticação de chaves e o gerenciamento de certificados utilizando *XML Key Management Specification (XKMS 2.0)* conforme a ***Especificação Técnica*** do ***GT 2 - Segurança*** recomenda na ***Tabela 8 – Especificações para Segurança – Desenvolvimento de Sistemas.***
- Prover a assinatura digital utilizando *XML Signature Syntax and Processing (XMLsig)* conforme a ***Especificação Técnica*** do ***GT 2 - Segurança*** recomenda na ***Tabela 8 – Especificações para Segurança – Desenvolvimento de Sistemas.***

Segurança no nível de transporte:

- Prover a segurança utilizando o componente *Transferência de Dados em Redes Inseguras* conforme a ***Especificação Técnica*** do ***GT 2 - Segurança*** recomendada na ***Tabela 5 – Especificações para Segurança – Comunicação de dados.***

Mínimo de segurança recomendado:

- O mínimo segurança exigido para troca de informações entre as aplicações que utilizem Web Services com os protocolos HTTP ou SMTP é a utilização de segurança no nível de aplicação utilizando o componente *Transferência de Dados em Redes Inseguras* conforme a ***Especificação Técnica*** do ***GT 2 - Segurança*** recomendada na ***Tabela 5 – Especificações para Segurança – Comunicação de dados.***
- Os servidores que provem serviços de Web Services deverão utilizar Certificado Digital da AC-raiz nos padrões da ICP-Brasil para que se possa garantir de autenticidade das informações trocadas entre as partes.
- Para serviços que necessitem de autenticação como usuário, senha ou qualquer outro mecanismo de autenticação, recomenda-se que tal informação seja transportada de forma criptografada na sessão de HEADER quando houver a utilização do protocolo de acesso SOAP.