Um Modelo de Composição de Políticas de Qualidade de Proteção para Serviços *Web* Compostos

Davi da Silva Böger, Michelle Wangham, Joni da Silva Fraga, Paulo Manoel Mafra
dsboger@gmail.com
http://www.das.ufsc.br/gcseg

1 de setembro de 2008

Tópicos

Introdução

- A Internet provê uma poderosa infra-estrutura de comunicação
- Possibilita o surgimento de aplicações distribuídas complexas
- Aplicações transpassam os limites de uma única organização
- Sistema aberto → Procupações com **interoperabilidade** e **segurança**

Introdução

Serviços *Web*

- Interoperabilidade:
  - Seguem a SOA
  - Baseados em padrões efetivos: XML, HTTP
  - Auto-descritos: WSDL, *WS-Policy*
- Segurança:
  - *WS-Security*, *WS-Trust*, *WS-SecureConversation*, ...
  - Políticas: *WS-SecurityPolicy*

- Facilitam a composição de aplicações (**Serviços Web Compostos**)

Introdução

Serviços *Web* Compostos

Serviços *Web* de diversas organizações interagem para realizar uma função de negócio (**Processo de Negócio**)

Duas formas de criar Serviços *Web* compostos

- **Orquestração**
  - Visão centralizada no *orquestrador*
  - Padrão W3C: WS-BPEL (*Recommendation*)
- **Coreografia**
  - Visão distribuída entre todos os participantes
  - Padrão W3C: WS-CDL (*Candidate Recommendation*)

Introdução

Segurança em Serviços *Web* Compostos

- Organizações diferentes:
  - Mecanismos e tecnologias de segurança diferentes
  - Possivelmente incompatíveis
- WS-BPEL e WS-CDL não tratam de aspectos de segurança
- Incompatibilidade de requisitos → Falha no processo de negócio

Proposta

Verificar, **antes da execução**, se os requisitos de segurança são compatíveis

Introdução

Objetivo

Desenvolver um modelo para determinar, antes da execução do processo de negócio, se há compatibilidade entre os requisitos de segurança dos Serviços *Web* envolvidos

- Baseado nos padrões de SW
  - Políticas de qualidade de proteção: *WS-Policy*, *WS-SecurityPolicy*
  - Linguagens de composição: WS-BPEL e WS-CDL
- Resultado: **política composta** do processo de negócio

Políticas em Serviços *Web*

Padrão *WS-Policy*

- Políticas expressam requisitos e capacidades de Serviços *Web*
- São anexadas a descrições WSDL
- Políticas são coleções de alternativas de política
- Alternativas de política são coleções de asserções de política
- Asserções de política descrevem comportamentos requeridos ou suportados pelo Serviço *Web*
  - São específicas de domínio
  - Definidas em outras especificações (*WS-SecurityPolicy*)
- A intersecção de duas políticas é a coleção de alternativas compatíveis pertencentes a ambas

Exemplo de política WS-Policy

```
1  <wsp:Policy wsu:Id="Policy1">
2     <wsp:ExactlyOne>
3        <wsp:All>
4           <sp:SignedParts>
5              <sp:Body />
6           </sp:SignedParts>
7        </wsp:All>
8        <wsp:All>
9           <sp:SignedParts>
10             <sp:Body />
11          </sp:SignedParts>
12          <sp:EncryptedParts>
13             <sp:Body />
14          </sp:EncryptedParts>
15       </wsp:All>
16    </wsp:ExactlyOne>
17 </wsp:Policy>
```


WS-SecurityPolicy

Asserções que descrevem:

- Partes de uma mensagem que serão protegidas
- Algoritmos de cifragem/assinatura/*hash*
- Parâmetros para esses algoritmos
- Tipos de credenciais (*tokens*)
- Ordenação das ações, *timestamps*, *layout*

- Não abrange controle de acesso
- Chamaremos de **Políticas de Qualidade de Proteção**

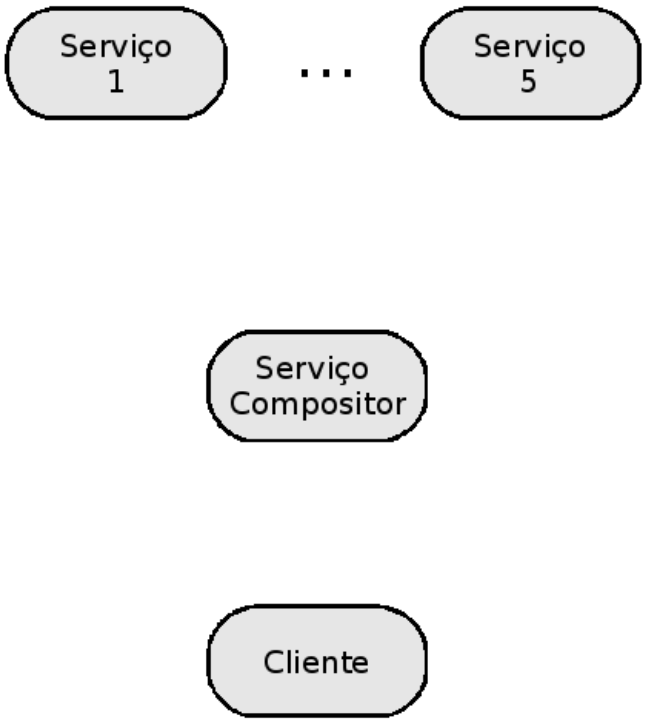
Modelo Proposto

Modelo Proposto

Calcula a **política composta** do **processo de negócio**

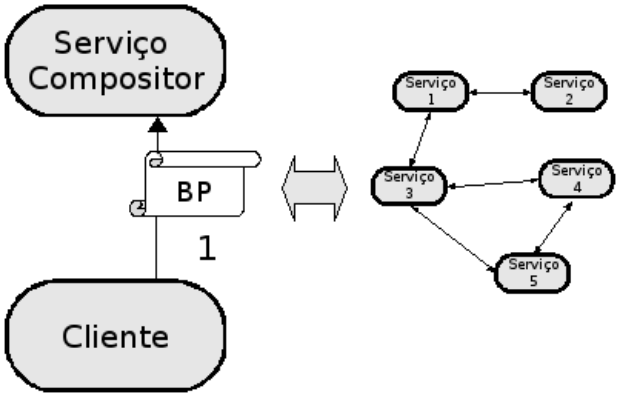
- Processo de negócio
  - Composto de um conjunto de trocas de mensagens
  - Participantes podem declarar políticas de qualidade de proteção
- Política composta
  - Contém uma política para cada troca de mensagem do processo
  - Intersecção das políticas anexadas à mensagem
  - Expressa a (in)compatibilidade dos requisitos de segurança
  - Indica quais mecanismos de segurança usar em cada troca de mensagem

Modelo Proposto

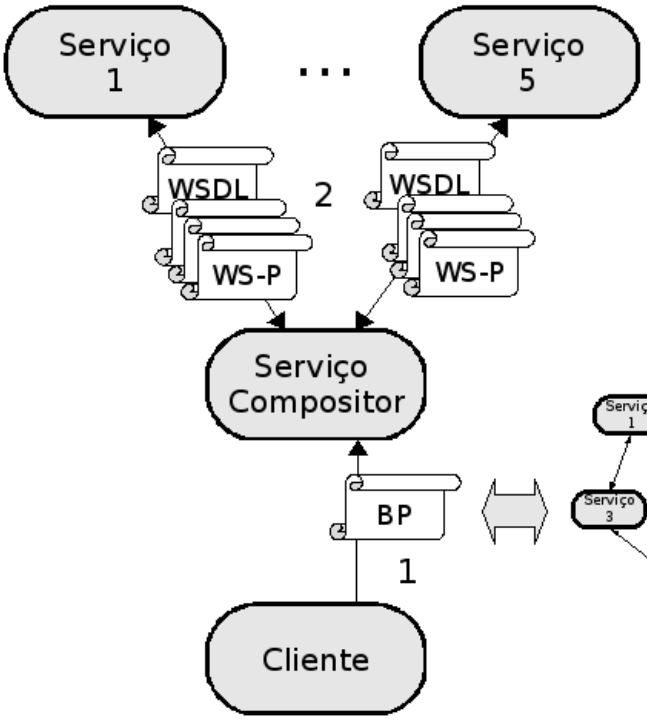


Modelo Proposto

1. Analisar a descrição do processo de negócio e identificar os Serviços *Web* participantes

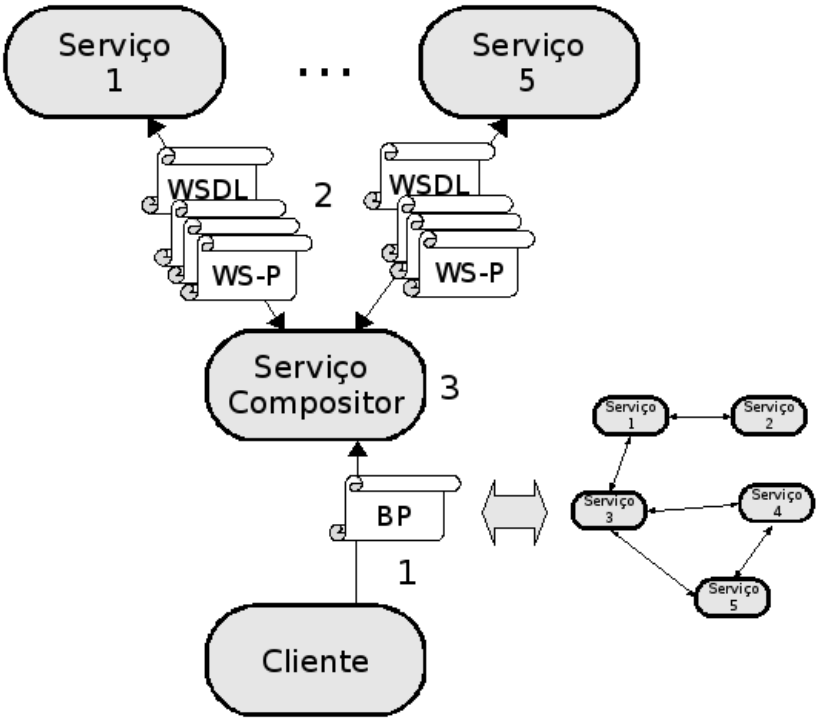


Modelo Proposto



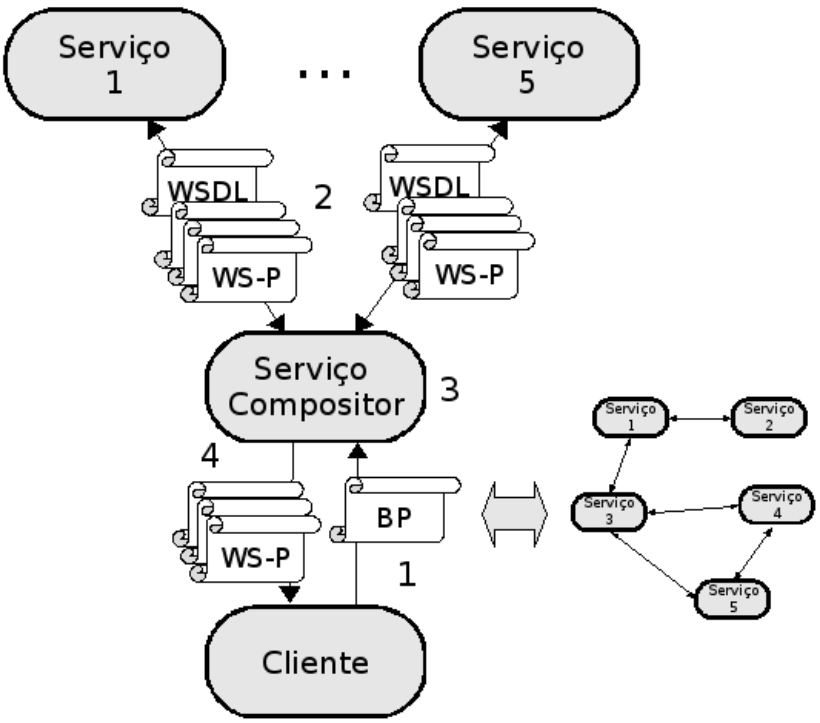
2. Obter as WSDLs e as políticas dos participantes

Modelo Proposto



3 Calcular a política composta

Modelo Proposto



4 Construir a resposta e enviar ao cliente

Passo 1 - Identificar processo e participantes

- Análise sintática da descrição do processo
- Participantes em um processo
  - WS-BPEL: orquestrador + *partner links*
  - WS-CDL: *role types*
  - Para o Serviço Compositor, o que importa são os *endpoints*
- *Endpoints* podem ser estabelecidos dinamicamente
  - Não é possível saber suas políticas antes da execução

Passo 2 - Obtenção das WSDLs e políticas

- WSDLs e políticas podem ser incluídas na requisição
- Se não, algum meio de obtê-las deve estar declarado
  - Endereços URL
  - Protocolo de troca de metadados: *WS-MetadataExchange*

Passo 3 - Cálculo da política composta

- Processo de negócio é decomposto em um conjunto de trocas de mensagens
  - WS-BPEL: *receive*, *invoke**, *reply*, *pick* e *onEvent*
  - WS-CDL: *exchanges* contidas em *interactions*
- Para cada troca de mensagem:
  - Identificar operação invocada
  - Identificar provedor e cliente
    - Se algum for dinâmico, troca de mensagem é marcada como dinâmica
  - Identificar as políticas que se aplicam à troca de mensagem
    - Explicado no próximo *slide*
  - Interseccionar a política do provedor com a política do cliente
  - Anexar a intersecção resultante à troca de mensagem

Passo 3 - Cálculo da política composta

Identificação das políticas

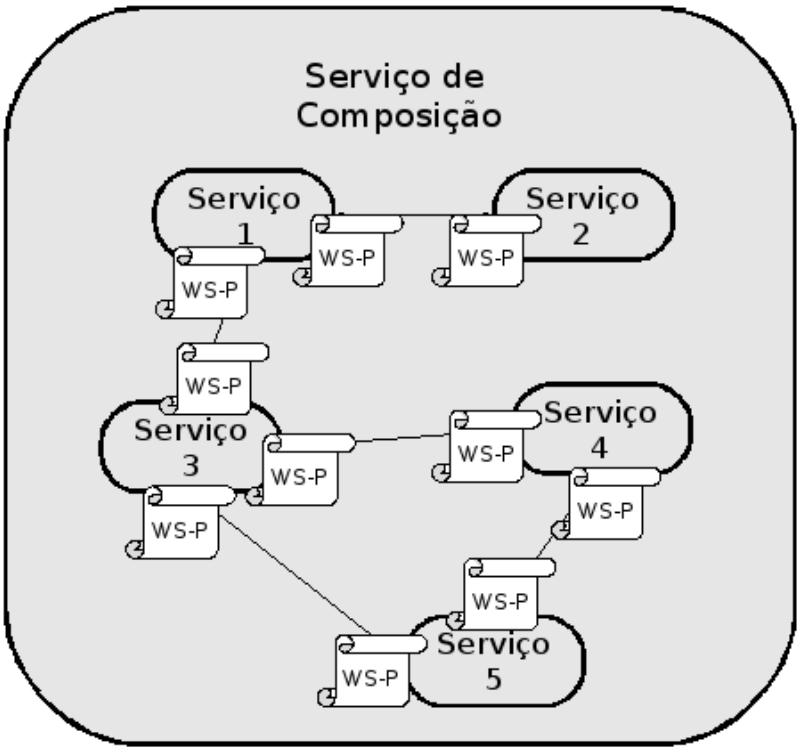
- Política do provedor é aquela anexada à sua WSDL
  - Total flexibilidade, pode ter uma política diferente para cada mensagem
- Cliente precisa expressar suas restrições
  - Usar política anexada ao *endpoint* (Muito restritivo)
  - Definir um novo sujeito de política (Solução adotada)
    - Cliente participante: representa a participação de um Serviço *Web* como invocador de operações em um processo de negócio

Passo 4 - Resposta

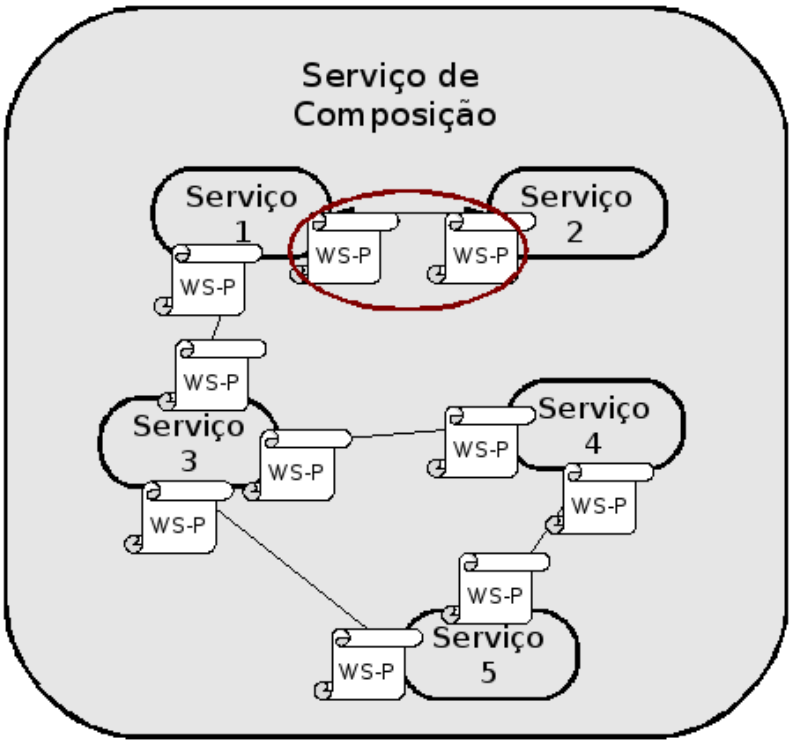
Resposta contém:

- Política composta
- Trocas de mensagens dinâmicas
- Resultado sumário
  - **Sucesso** - Nenhuma incompatibilidade, Nenhuma troca dinâmica
  - **Falha** - Alguma Incompatibilidade
  - **Inconclusivo** - Nenhuma incompatibilidade, Alguma troca dinâmica

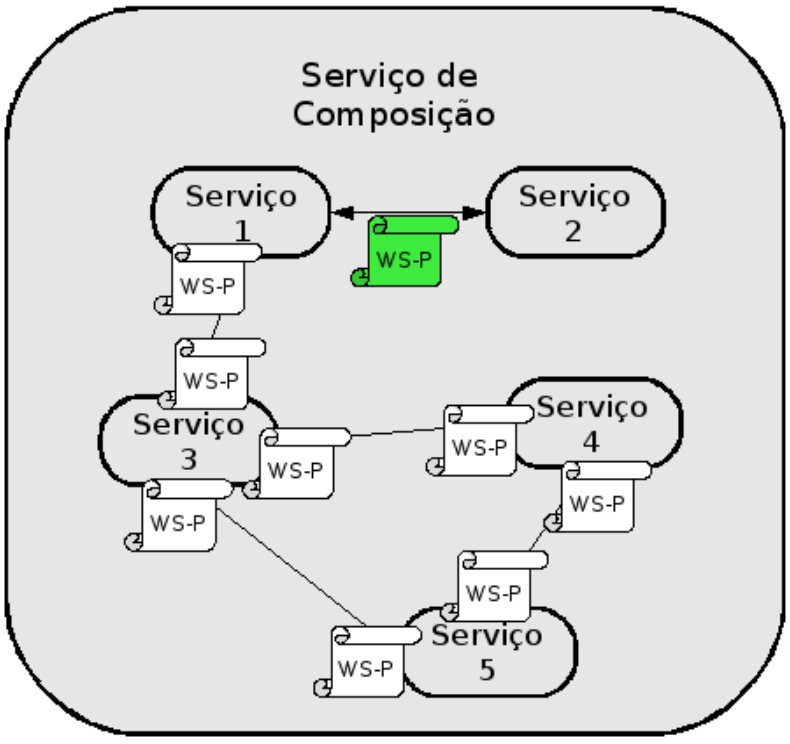
Ilustração



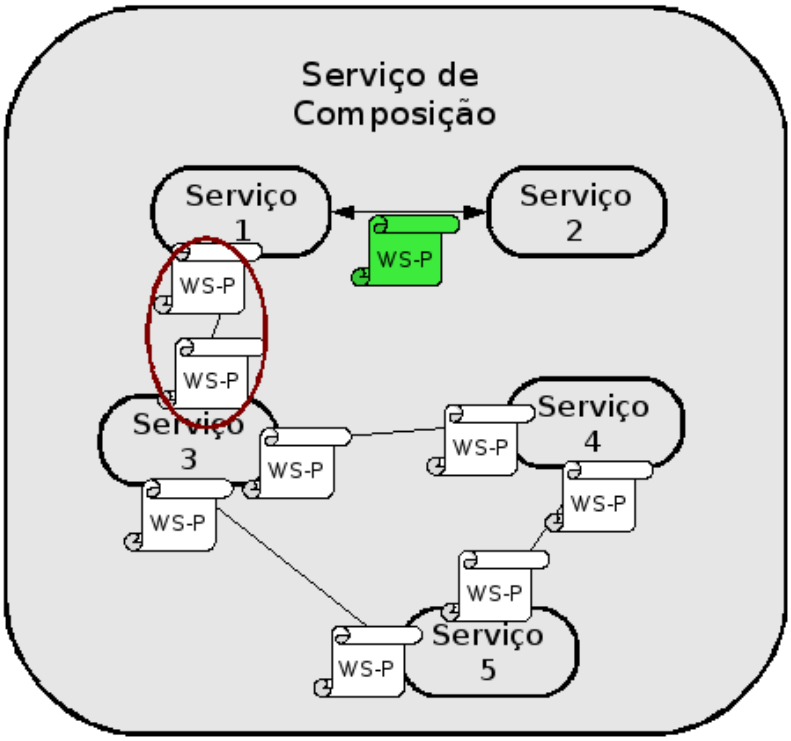
Ilustração



Ilustração

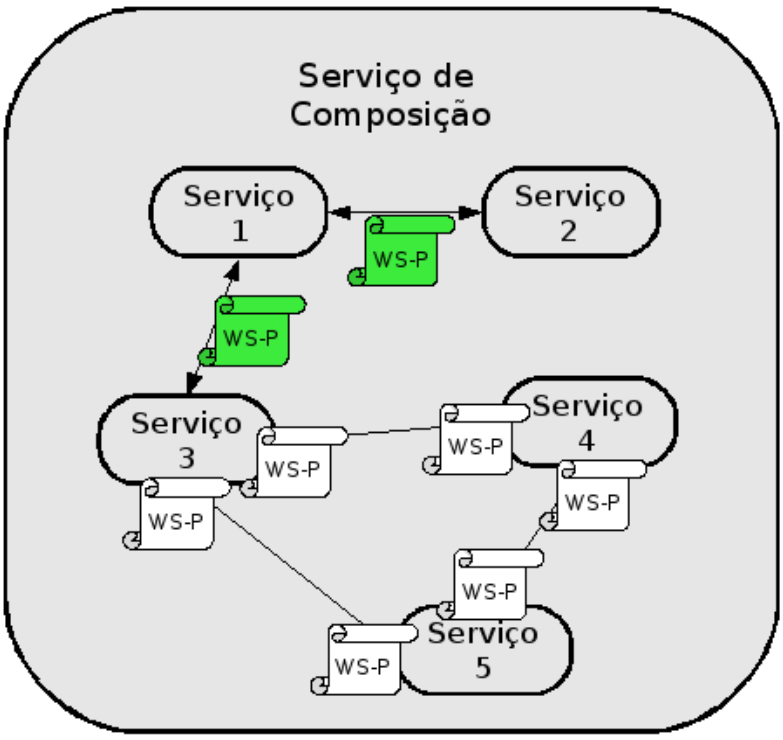


Ilustração

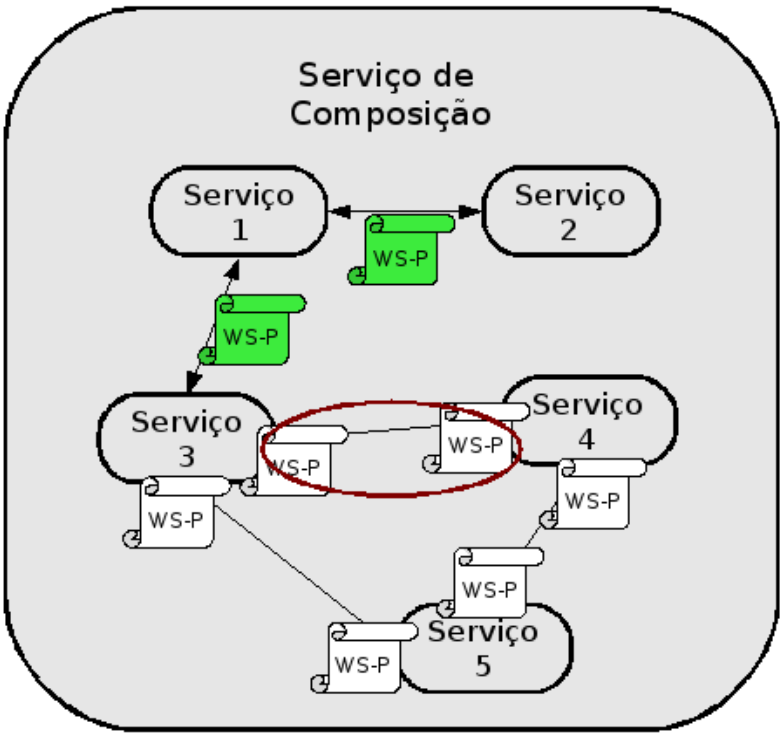


Um Modelo de Composição de Políticas de Qualidade de Proteção para Serviços *Web* Compostos
└Modelo Proposto

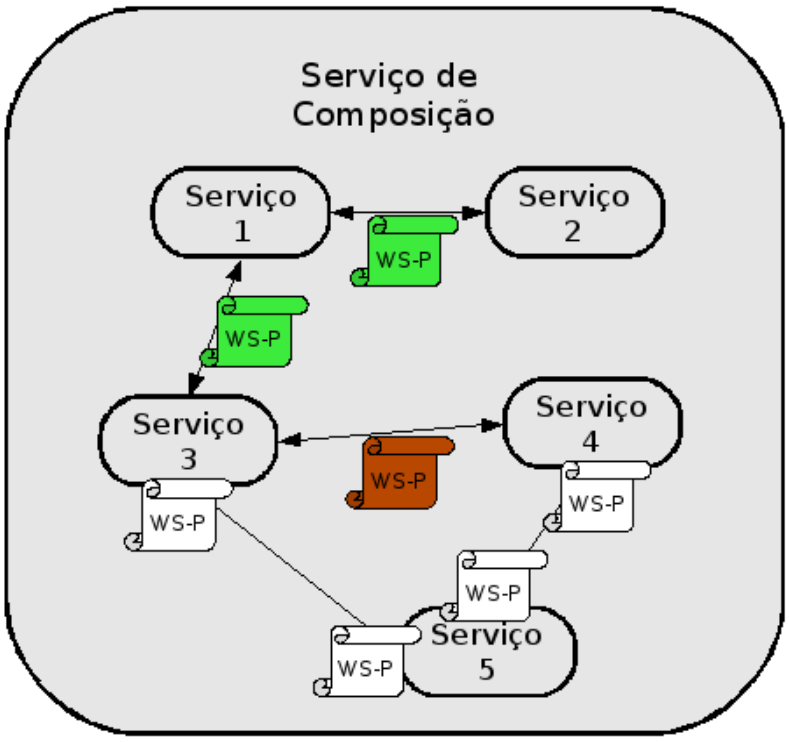
Ilustração



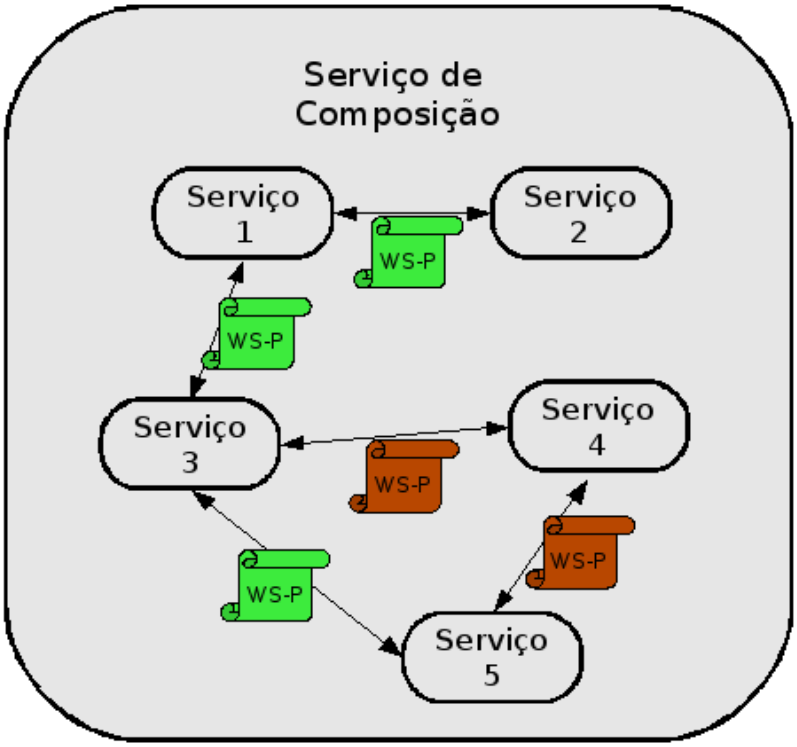
Ilustração



Ilustração



Ilustração



Implementação

Ferramentas e bibliotecas usadas

- Linguagem Java
- *Eclipse* (3.3.0)
- *JUDE Community* (5.2.1)
- *JUnit* (3)
- *Apache Tomcat* (6.0.7)
- *Apache Axis2* (1.3)
- *Apache Rampart* (1.3)
- *Apache ODE* (1.1.1)
- *Sun WSDL4J* (1.6.2)

Implementação

Funcionalidades suportadas no protótipo

- Processar políticas *WS-Policy*
- Identificar anexos de política em descrições WSDL 1.1 (WSDL 2.0 ainda não suportada)
- Obter as interfaces WSDL e as políticas por meio de URLs (*WS-MetadataExchange* ainda não suportado)
- Identificar as interações em processos WS-BPEL (processos WS-CDL ainda não são suportados)
- Cálculo da política composta

Implementação

- Inicialmente, a biblioteca *Apache Neethi* seria usada para processar políticas *WS-Policy*
- Mas esta não implementa nem intersecção de políticas, nem anexos

GWSPolicy - GCSeg WS-Policy Implementation

- Implementa toda a especificação *WS-Policy*
  - Exceto anexos em WSDL 2.0 e UDDI
- Independente do Serviço Compositor
- Distribuída sob a GPL

Conclusão

- Foi desenvolvido um modelo que realiza a composição de políticas de qualidade de proteção em Serviços *Web* compostos
  - Baseado em padrões consolidados
  - Suporta tanto WS-BPEL quanto WS-CDL
- Um subconjunto substancial do modelo foi implementado no protótipo
- Foi desenvolvida uma implementação da *WS-Policy*
- Ambos foram desenvolvidos para serem flexíveis, extensíveis e conforme os padrões
- Em breve, mais informações em www.das.ufsc.br/gcseg

Trabalhos futuros

- Estender o protótipo do Serviço Compositor a todas as funcionalidades do modelo
- Promover a resolução dinâmica das incompatibilidades identificadas na política composta
  - Técnicas de transposição de tecnologias de segurança
  - Técnicas baseadas em terceira parte confiável
  - ...

Obrigado!

Perguntas?