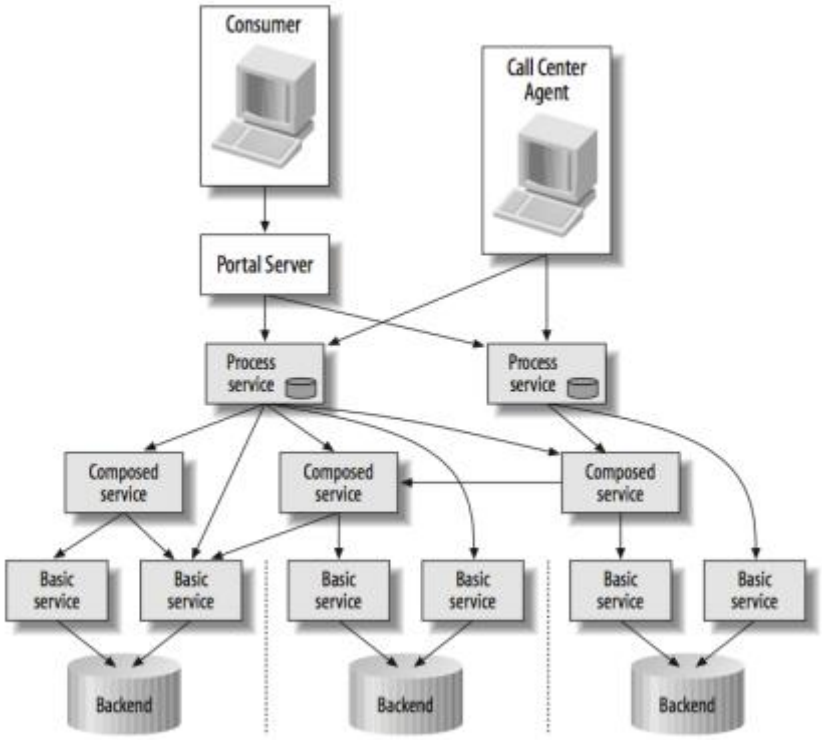
5- Rendimiento y Seguridad

Seguridad

1. Sea el siguiente sistema, en el que el consumidor puede comenzar un proceso a través de un portal de servicios:



Dicho proceso podría ejecutarse en distintas capas (distintos procesos de servicio, servicios compuestos o servicios básicos). Esta multitud de capas lleva a dos problemas importantes:

1. No está claro qué sistema autentica y autoriza al usuario
2. La confidencialidad debe asegurarse a través de no una sino múltiples conexiones y nodos intermedios.

Sobre el punto 1, reflexiona sobre por qué no está claro qué sistema autentica a un usuario y autoriza sus actividades. Es responsabilidad del backend, del frontend, de ambos?

Sobre el punto 2, ¿es suficiente para garantizar la confidencialidad e integridad que las conexiones físicas punto a punto sean seguras? ¿Por qué? Si transferimos datos sensibles como contraseñas, números de cuenta bancaria, etc. ¿qué entidades/procesos deberían poder ver dicha información y cuáles no?

[Fuente original: Jossutis 2007 , SOA in Practice, Fig. 14-1]

2. ¿Es posible que haya partes de un sistema orientado a servicios sin seguridad?

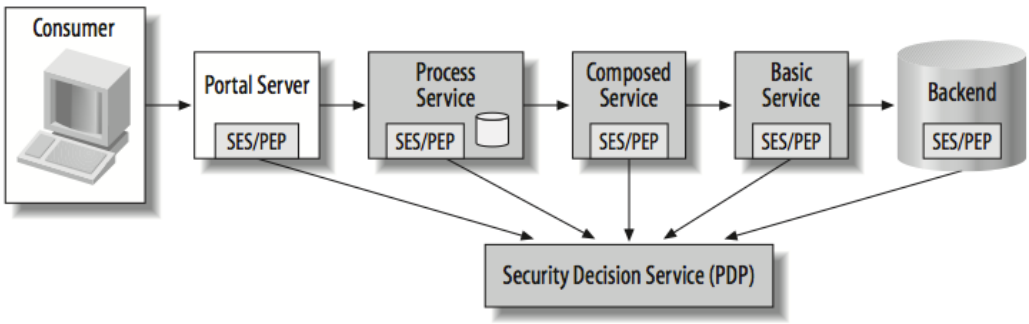
Sea un servicio que retorna datos de clientes a cada consumidor. Existen clientes VIP cuyos datos no queremos que sean visibles a cualquier consumidor. ¿Cómo podríamos implementar un sistema de seguridad para evitarlo? ¿Se te ocurre alguna forma de hacerlo en la capa de negocio?

3. ¿Podemos asumir, en general, que las distintas infraestructuras que utilizamos (Internet, servicios web o cualquier otro middleware) tratan con la seguridad de tal modo que no necesitamos preocuparnos por ella?

¿La mayoría de los estándares abiertos para servicios web (XML, SOAP, WSDL, etc.) tienen un soporte conceptual de la seguridad en sus definiciones?

4. ¿Cuál es la capa donde es más sencillo introducir seguridad punto final a punto final? Razona tu respuesta con algún ejemplo.

5. Imaginemos un sistema en que la seguridad se ha implementado como un servicio más, de tal modo que distintas entidades (servicios, backends, frontends) pueden consultarlos para tomar decisiones respecto a la seguridad, por ejemplo:



Este 'Security Decision Service', o más comúnmente llamado idP (identity Provider) provee decisiones sobre seguridad, acceso o política a aplicar a los datos. La Kantara Initiative, por ejemplo, busca dar servicios de identidad genéricos en Internet.

¿Qué problemas o ventajas le ves a este sistema respecto a otros, como implementar la seguridad en la capa de mensajes o de transporte?

6. Las expresiones XPath permiten evaluar condiciones dentro de un XML. Por ejemplo, la siguiente línea comprueba que un nombre de usuario y una clave coinciden con la información de una cuenta en una base de datos XML:

```
string(//user[name/text()='user' and password/text()='pw']/account/text())
```

La base de datos tiene el siguiente aspecto:

```
<user>
     <name>josuttis</name>
          <password>secret77</password>
          <account>admin</account>
     </name>
```

```
<name>
...
</name>
```

¿Cómo podríamos utilizar una inyección XPath para burlar la comparación de que el nombre del usuario y el texto de la contraseña coincidan?. Buscad una inyección que sólo requiera cambiar `'user'` por una expresión que burle la seguridad.