



# Webapplicatie beveiliging met externe authenticatie agents

Marcel Ammerlaan

**I PROFS**  
The Java Company

# Inhoud

- J2EE standaard Web beveiliging
- Access Managers voor J2EE
- DigiD
- Access Manager en DigiD
  
- Vragen?



**IPROFS**  
The Java Company

# J2EE Web Security

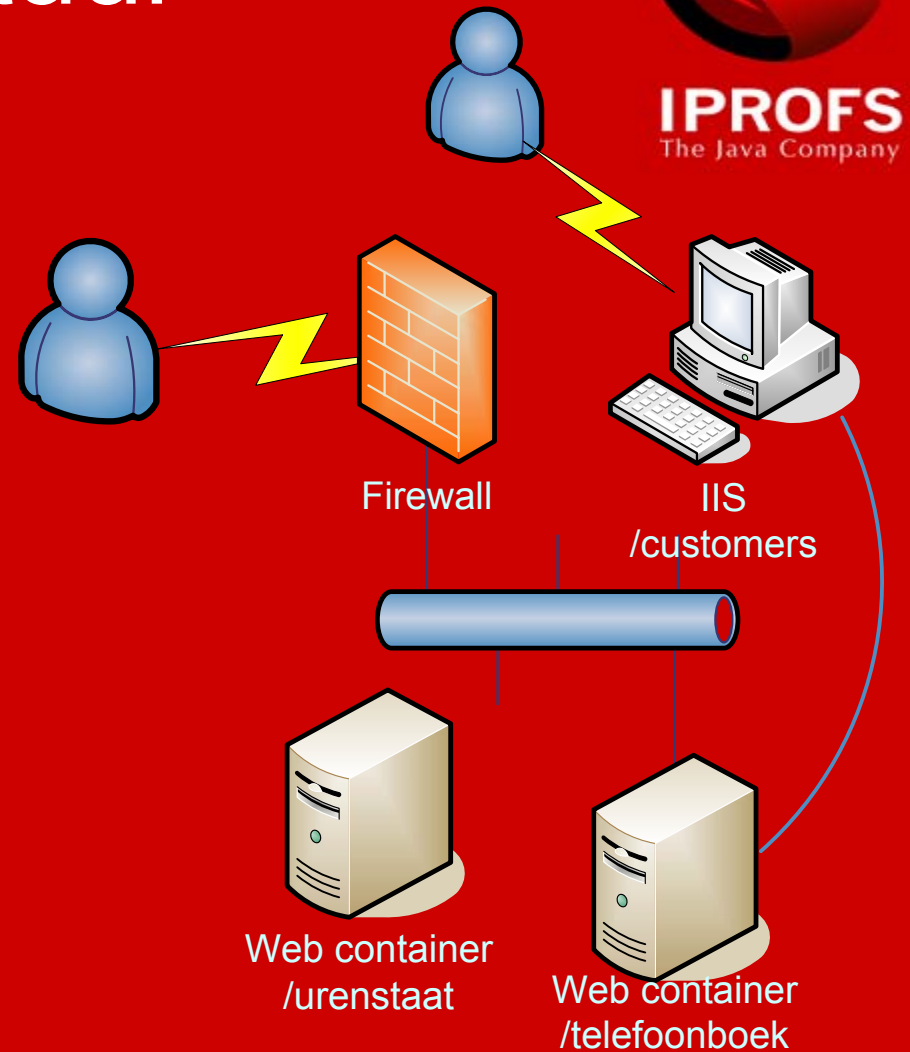


**IPROFS**  
The Java Company

- Authenticatie
  - Form
  - Basic
- Authorisatie
  - Role-based access
    - Vaak via een LDAP server
  - Per pad / methode
    - Beveiligde subdirectories
- API support
  - `isUserInRole()`, `getUserPrincipal()`, ...
- Andere zaken: data integriteit, confidentiality (niet behandeld)

# J2EE infrastructuur

- Basis opzet infrastructuur
- En (wild) groei..
- Nieuwe wensen
  - SSO
  - Security zones
  - Consolidatie
  - Security
- Simpele oplossingen:  
Meer programmeren  
Meer servers



# Web Security OWASP



**IPROFS**  
The Java Company

- Voor deze presentatie van belang
  - Unvalidated Input (paden in request parameters)
  - Improper error handling (stacktraces)
  - Broken access control (missing checks)
  - Broken authentication/authorisation (naam/wachtwoord in URL)
  - Denial of service (backend overload)

# Access Manager



**IPROFS**  
The Java Company

## Uitgangspunten:

- **Authenticatie uit de applicatie**
  - Centrale systemen zijn eenvoudiger in beheer
- **Fijnmaziger authorisatie**
  - Tijd, source ip adres,
- **Integratie met diverse platformen**
  - J2EE, Windows
- **Federatie**
  - Meerder sites, 1 URL
- **Step-up authenticatie**
  - Iedere applicatie zijn eigen niveau van beveiliging
- **Identity management**

# Access Manager (2)



**IPROFS**  
The Java Company

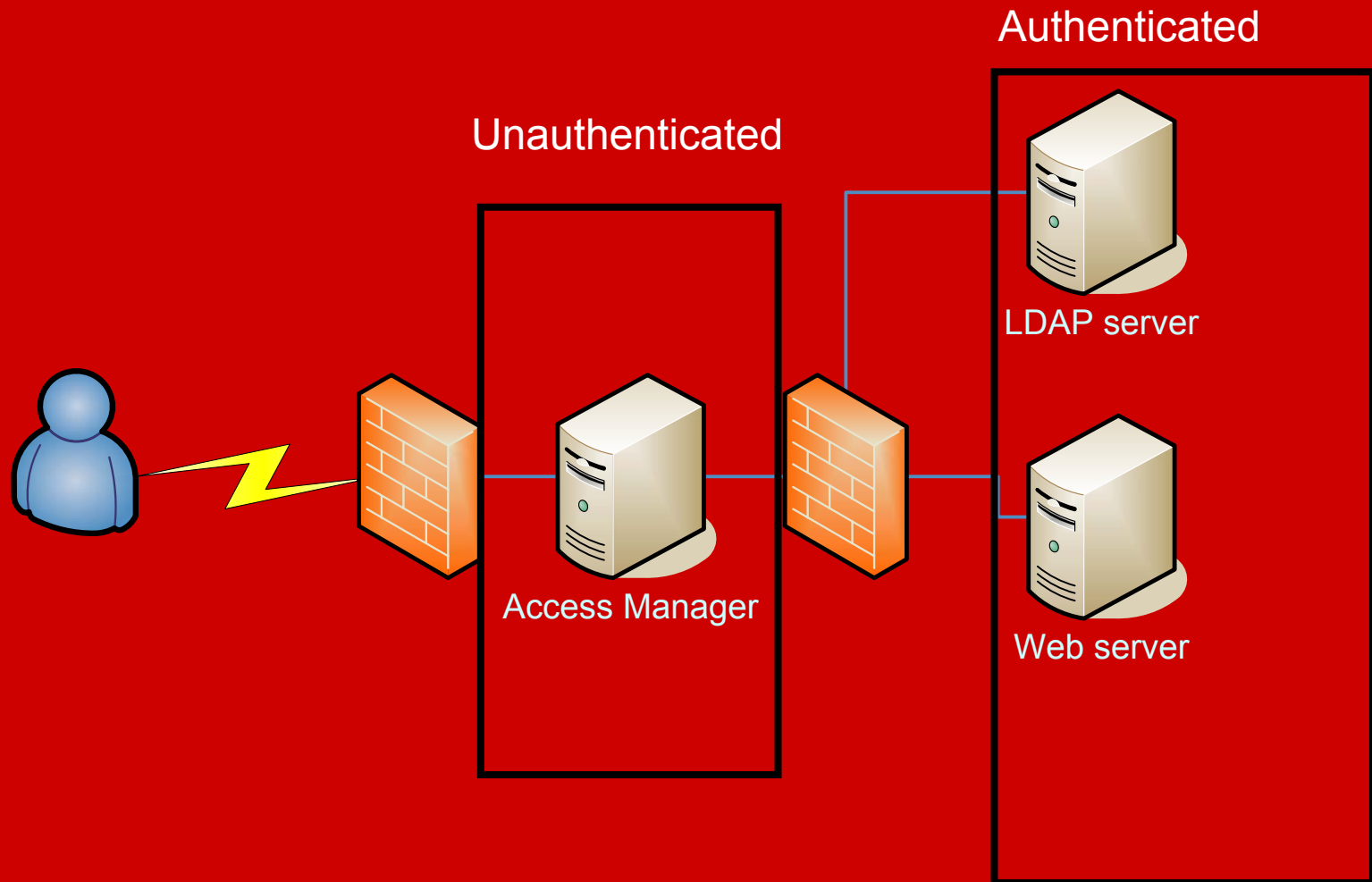
## Producten

- IBM Tivoli Access Manager
  - Sun Access Manager
  - Josso (Open source)
  - WebFederate
- 
- Deze presentatie gaat niet over 1 specifiek product. Sommige features zitten niet in ieder product
    - Alles zit in potentie in Josso (Open Source)

# Infrastructuur met Access Manager



**IPROFS**  
The Java Company



# Implementatie



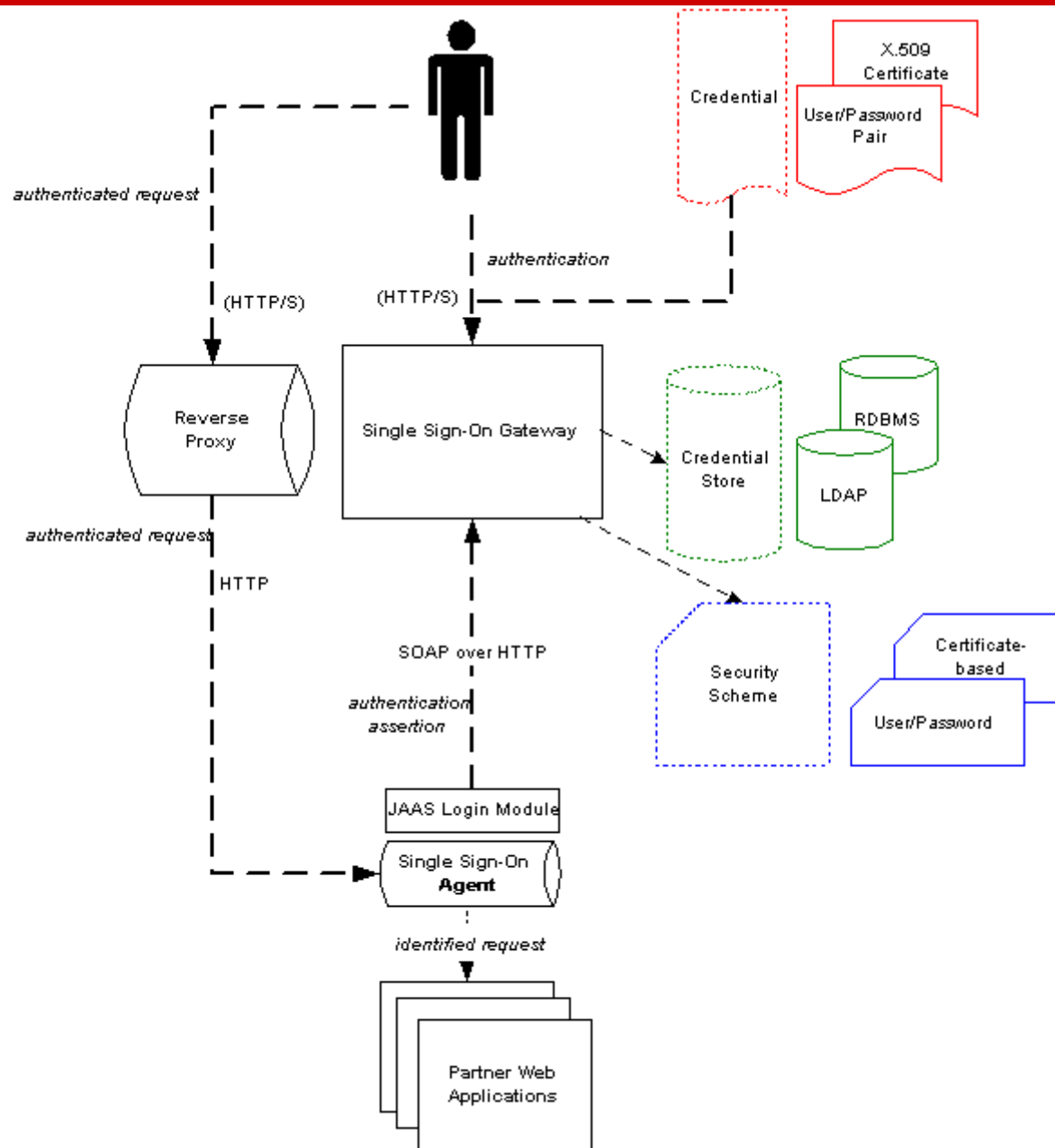
**IPROFS**  
The Java Company

- Access manager is een reverse HTTP proxy
- Zo min mogelijk in de DMZ: authorisatie via een losse server (authorisation of policy agent)



**IPROFS**  
The Java Company

# JOSSO implementatie



# Authenticatie



**IPROFS**  
The Java Company

- Reverse proxy kan (vaak) basic en form-based login
- Complexere login vereist een (losse) applicatie
  - Single-sign-on gateway in JOSSO termen
- Reverse proxy blijft verantwoordelijk voor de link met de applicatie
- Communicatie tussen de reverse proxy en sign-on gateway

# Koppeling met backend



**IPROFS**  
The Java Company

- IBM term: junction
- Persistente HTTP(S) connectie met de web-applicatie
- Security gegevens worden hierover doorgegeven
  - Basic authentication
  - Proprietary (leverancier specifiek: NTLM, LTPA, ...)
- Security niveau per junction
  - Step-up authentication

# Koppeling met backend (2)



**IPROFS**  
The Java Company

- Inkomende URL wordt gecontroleerd
- URL wordt vertaald naar interne URL
- Pagina wordt gehaald van de interne URL
- Interne links in de pagina worden vertaald naar externe URLs
- Pagina wordt teruggegeven

# Wat doet dit voor de applicatie?



- Niets!
- Nou ja....
- Impact van een reverse proxy
  - Links in de pagina's
    - HTML
    - Flash
    - Javascript
    - *href="http://interne.server.com/bla.html"*
    - Alles relatief helpt
  - Hogere performance (pipelining, persistent connections)
  - Protocol conversie (https→http)

# Wat doet dit voor de applicatie? (2)



- Federatie
  - <http://extern.bedrijf.com/customers/>
  - <http://intern.bedrijf.com/apps/customers/>
- Web context van de applicatie kan veranderen
  - Kan een behoorlijke impact hebben (onverstandig in de praktijk)

# Access Managers & OWASP



**IPROFS**  
The Java Company

- Unvalidated Input (paden in request parameters)
  - Op een junction kan een filter zitten
  - White-listing van geldige karakters
- Improper error handling (stacktraces)
  - Generieke error pages
- Broken access control (missing checks)
  - Niet meer het probleem van development ☺
- Broken authentication/authorisation (naam/wachtwoord in URL)
  - Access Managers worden gemaakt voor veilige authenticatie. Als dit al niet meer lukt...
- Denial of service (backend overload)
  - Throttling op de junction

# DigiD



**IPROFS**  
The Java Company

- *Bedrijven kunnen vanaf 25 november 2005 ook gebruik maken van DigiD. DigiD staat voor Digitale Identiteit, een gemeenschappelijk systeem van en voor de overheid.*
- *Bedrijven die DigiD willen gebruiken maken momenteel gebruik van de toegangscode van de Kamer van Koophandel.*

# DigiD (2)



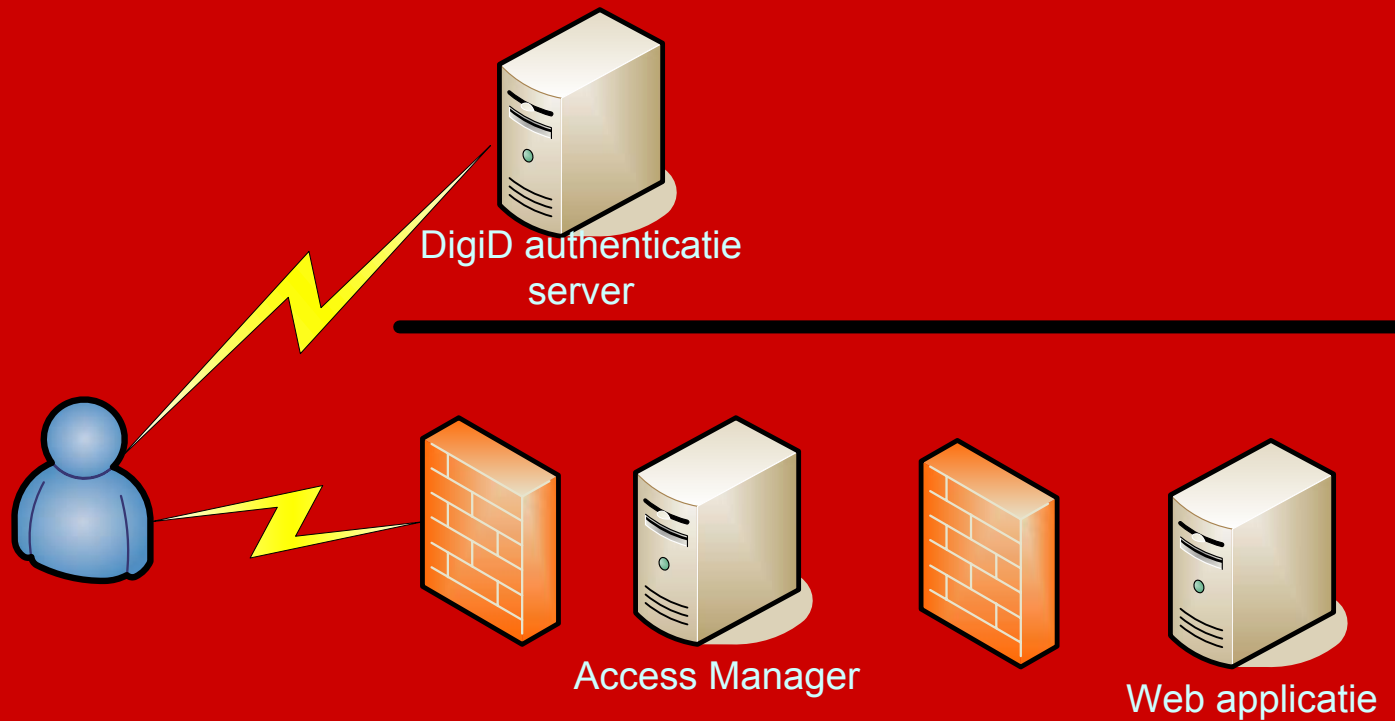
**IPROFS**  
The Java Company

- DigiD is een SSO omgeving
- Diverse authenticatie middelen mogelijk
- Veiligheids niveau per authenticatie server
- Ideaal om te integreren met een Access Manager!

# Integratie van DigiD



**IPROFS**  
The Java Company



# Ontwikkelen van DigiD access manager

- Op basis van WebFederate
  - Speciale klant wensen
- Gebruik makend van A-select
  - Agent en server omgeving
- Techniek zou overgenomen kunnen worden in JOSSO

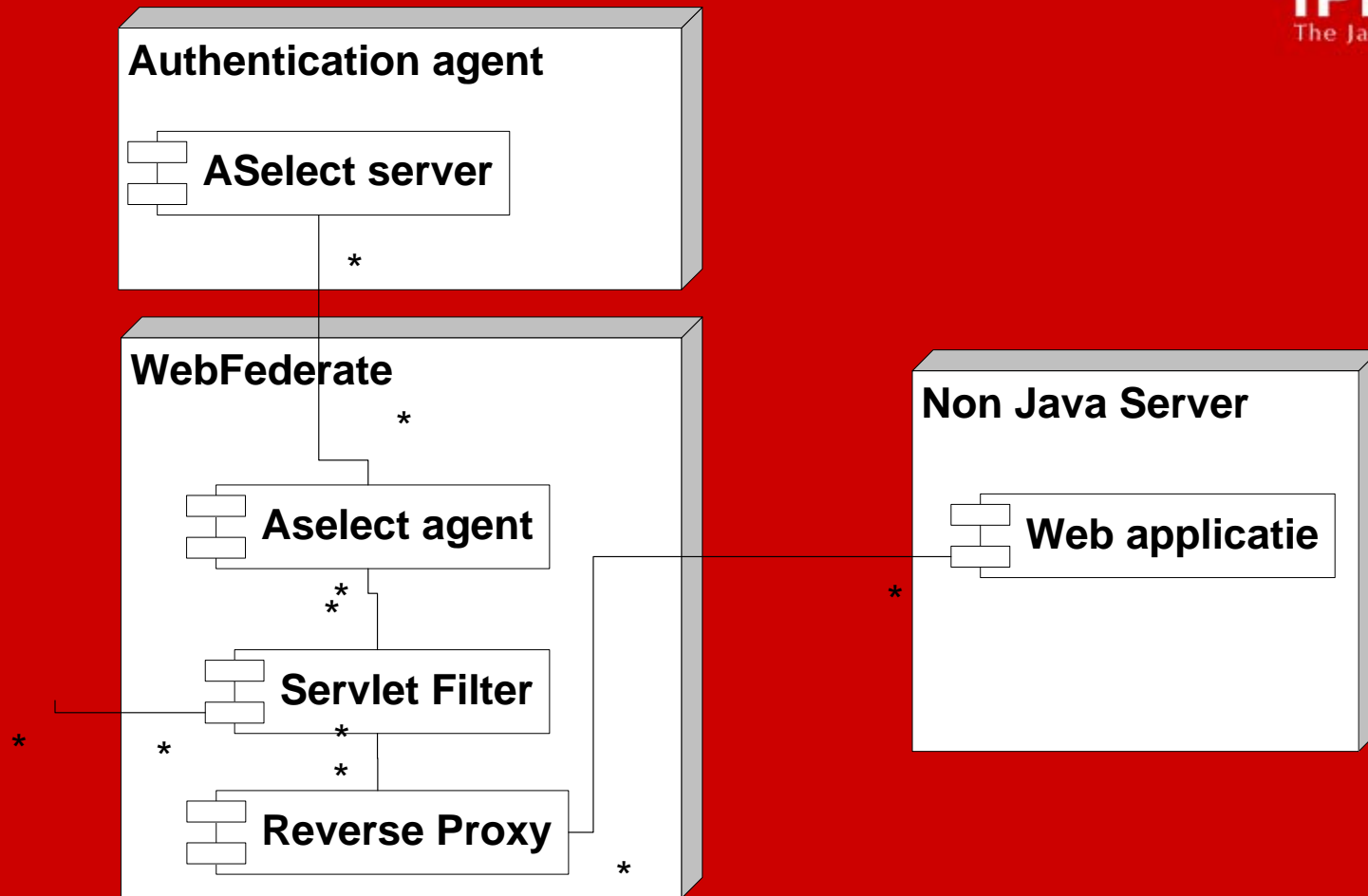


**IPROFS**  
The Java Company

# Ontwikkelen van DigiD access manager (2)



**IPROFS**  
The Java Company



# Het filter



**IPROFS**  
The Java Company

```
if(filt.authentication(req,
    res)) {
    String user=filt.getOtvSsn(req)
    chain.doFilter(req, res)
} else {
    res.setStatus(HttpServletResponse.SC_FORBIDDEN)
}
```

# De proxy



**IPROFS**  
The Java Company

```
public void doGet(HttpServletRequest req, HttpServletResponse res) {  
    URL back = new URL("http://back/" +  
        req.getRequestURI().substring(...));  
    String s = back.getContent();  
    s.replace("...", "...");  
    res.getWriter().write(s);  
}
```

Vragen?

Zijn er nog vragen?

Contact info:  
[www.iprofs.nl](http://www.iprofs.nl)  
[info@iprofs.nl](mailto:info@iprofs.nl)