XML Signature Wrapping: Die Kunst SAML Assertions zu fälschen

Andreas Mayer
Adolf Würth GmbH & Co. KG
Künzelsau-Gaisbach

Prof. Dr. Jörg Schwenk
Lehrstuhl für Netz- und Datensicherheit
Ruhr-Universität Bochum

19. DFN Workshop „Sicherheit in vernetzten Systemen“
Hamburg, 22.02.2012

Agenda

- Motivation
- Grundlagen
- XML Signature Wrapping
- Angriff auf Shibboleth
- Gegenmaßnahmen
- Fazit

SAML in a nutshell

- Security Assertion Markup Language
- XML-basierte Auszeichnungssprache
- Austausch von Authentifizierungs- und Berechtigungsinformationen
- Offener Standard
- Einsatzgebiete
  - Browserbasiertes Single Sign-On
  - Webservices in SOA Architekturen

Wo wird SAML eingesetzt?

Microsoft® Office 365

SuisseID

amazon web services™

Der neue Personalausweis

Shibboleth®

Single Sign-On mit SAML

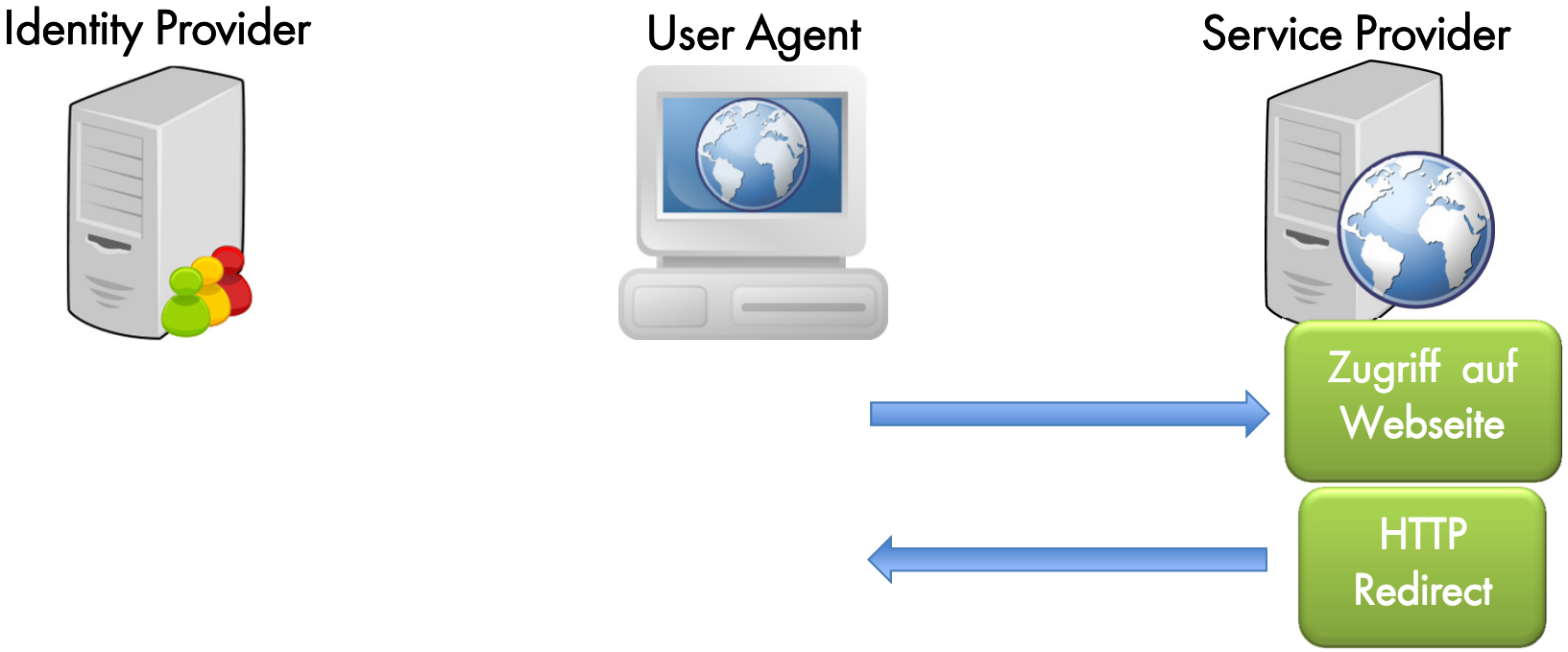
Identity Provider

User Agent

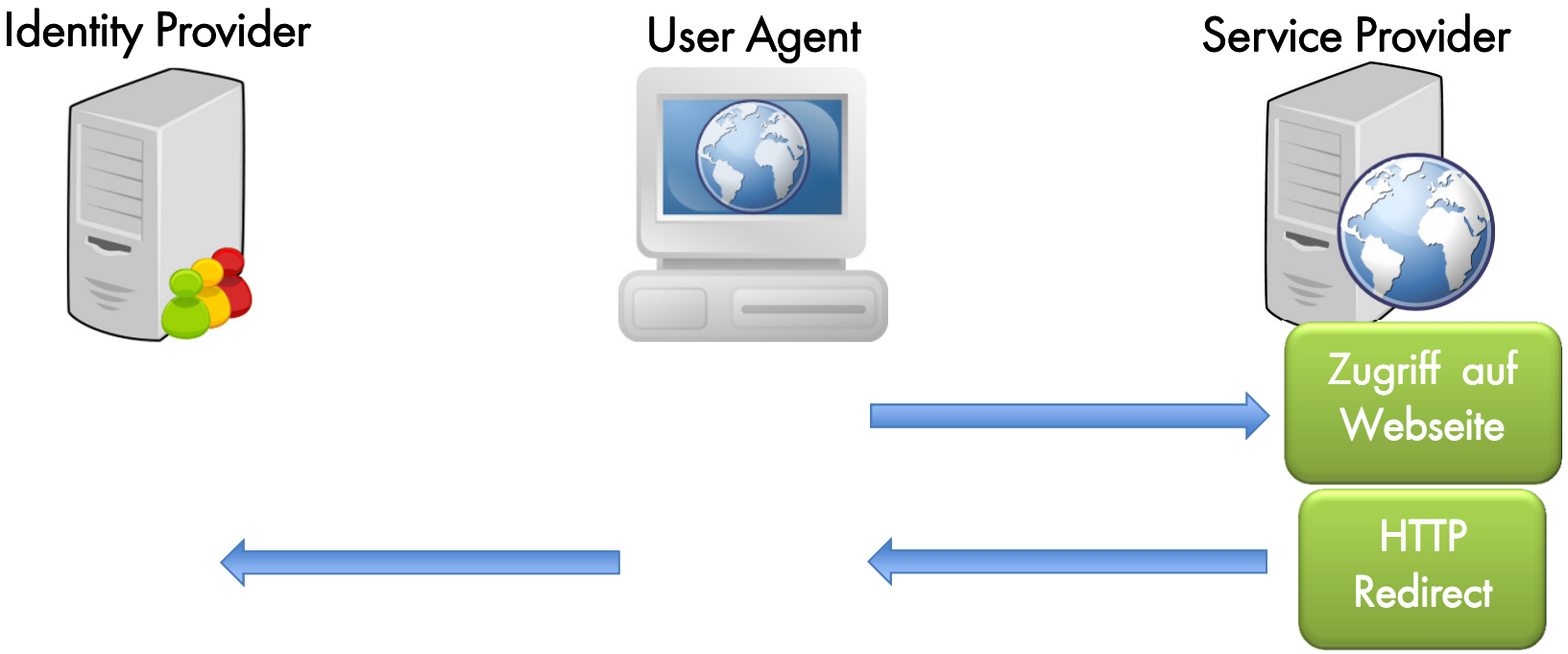
Service Provider

Single Sign-On mit SAML

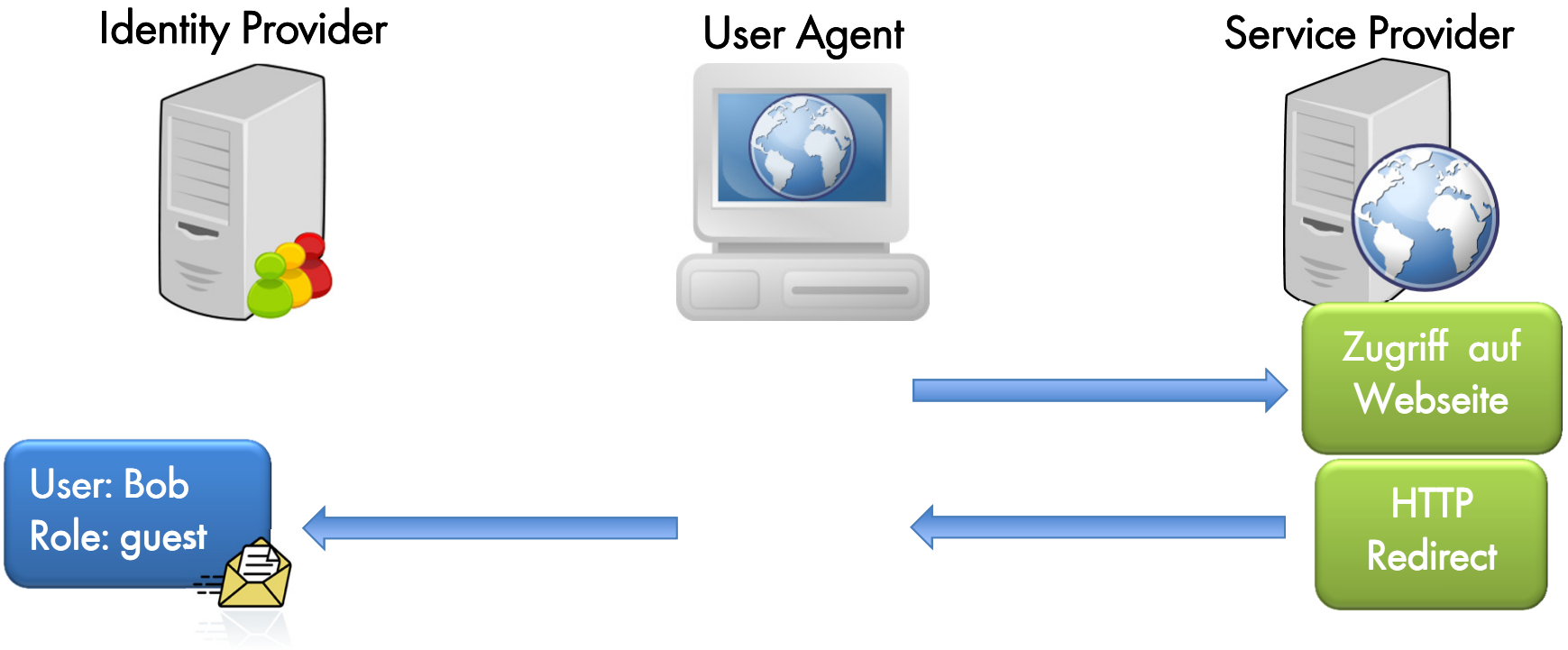
Single Sign-On mit SAML



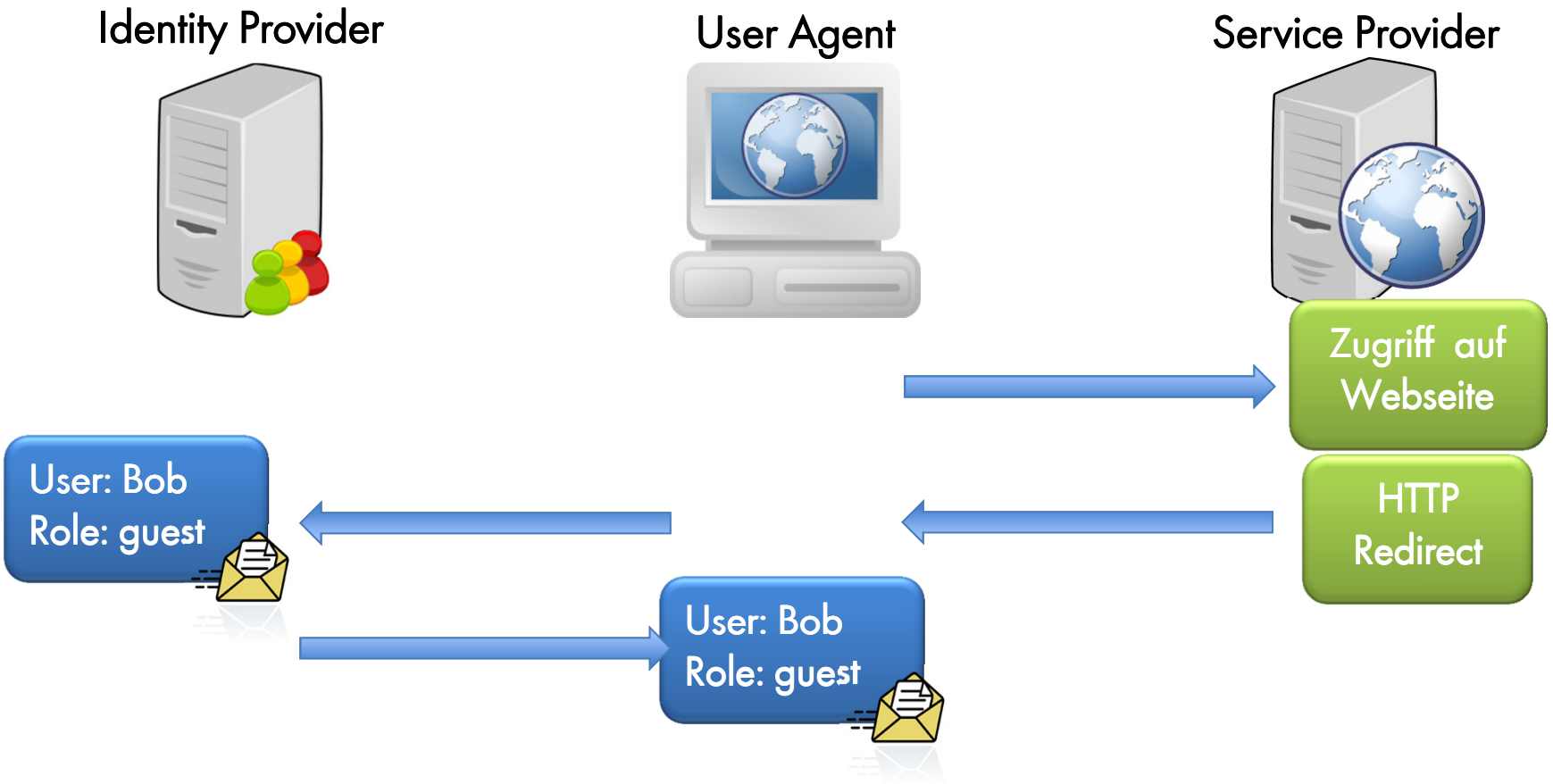
Single Sign-On mit SAML



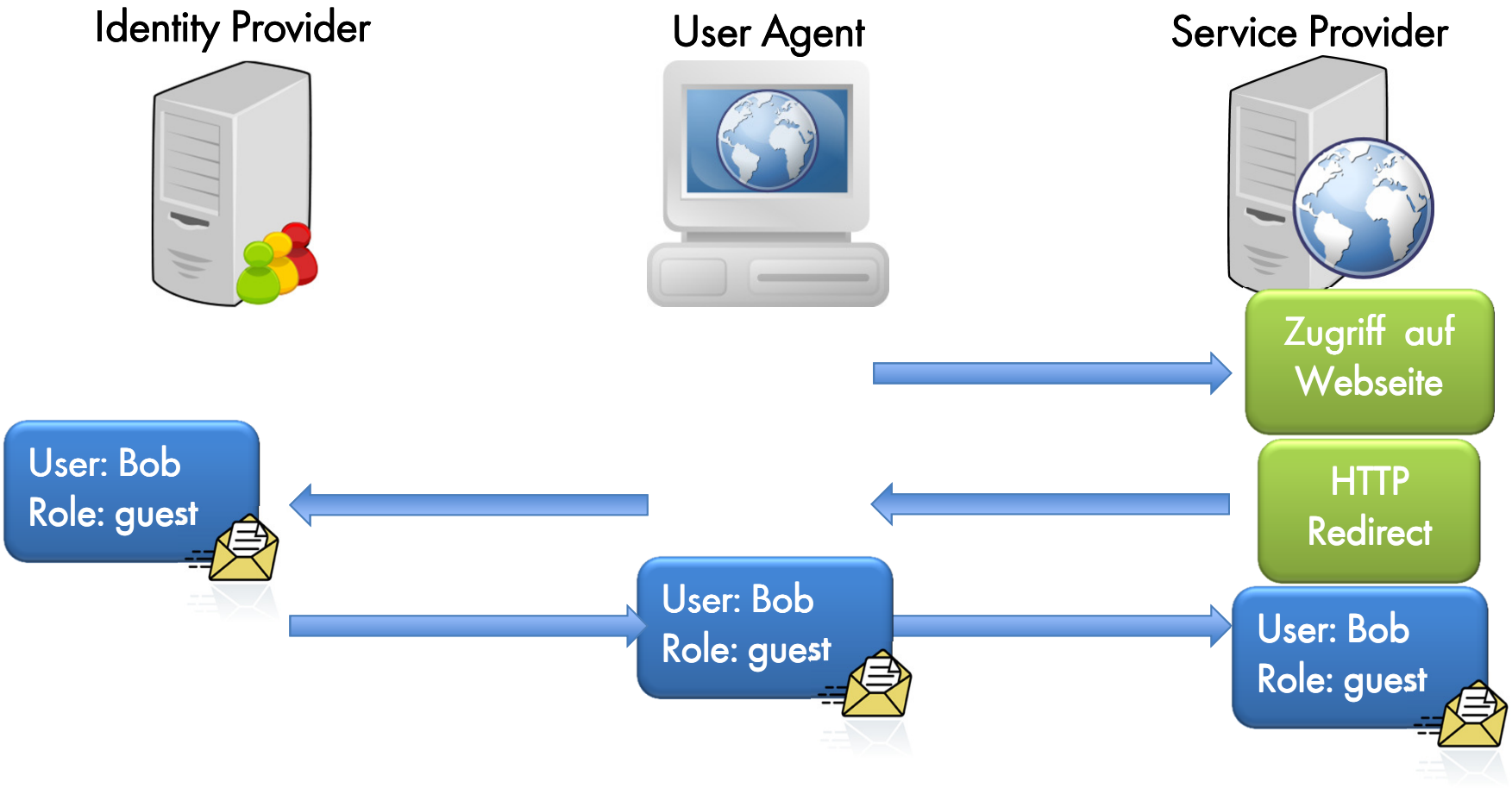
Single Sign-On mit SAML



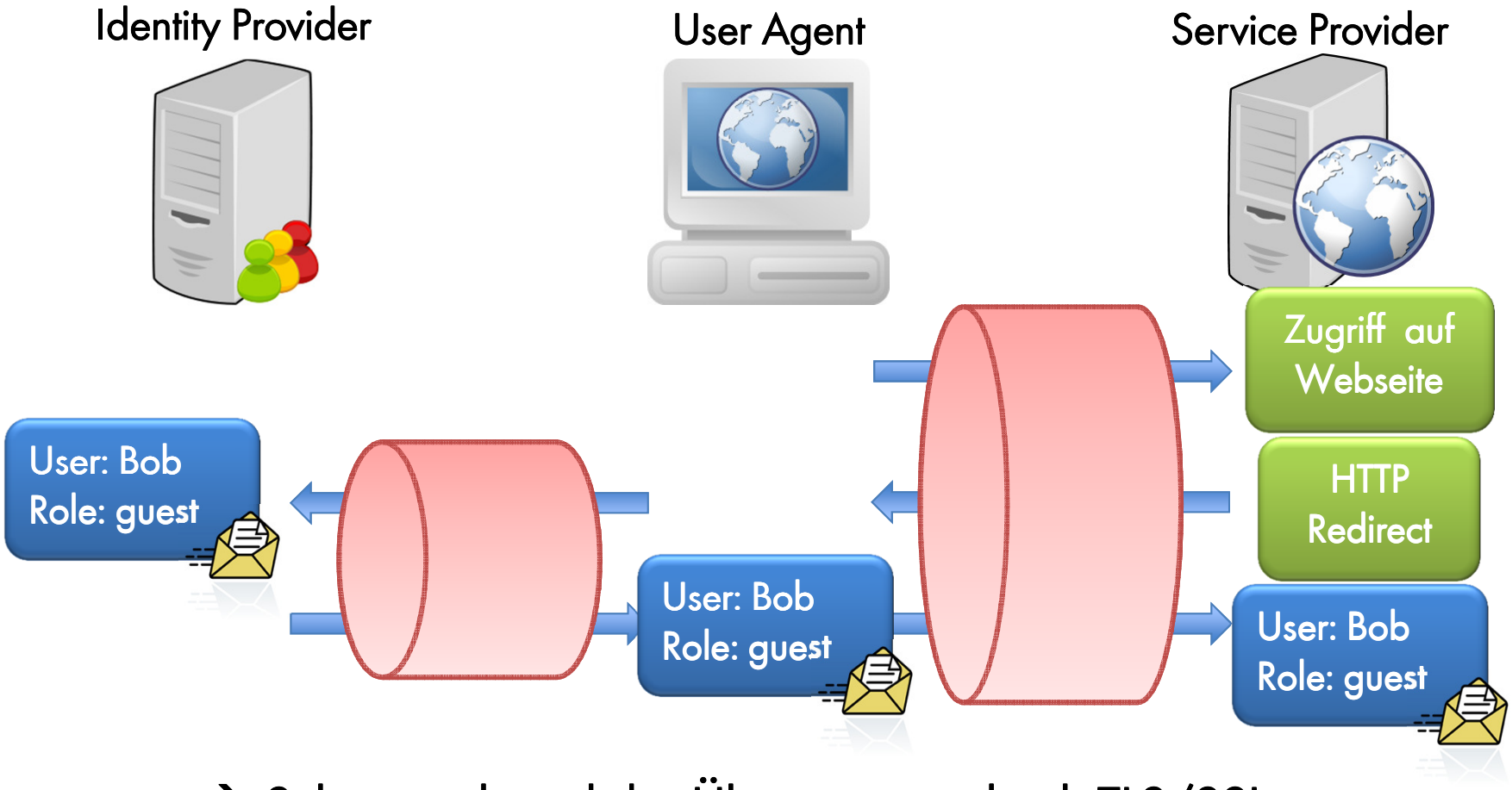
Single Sign-On mit SAML



Single Sign-On mit SAML



Single Sign-On mit SAML



→ Schutz während der Übertragung durch TLS/SSL

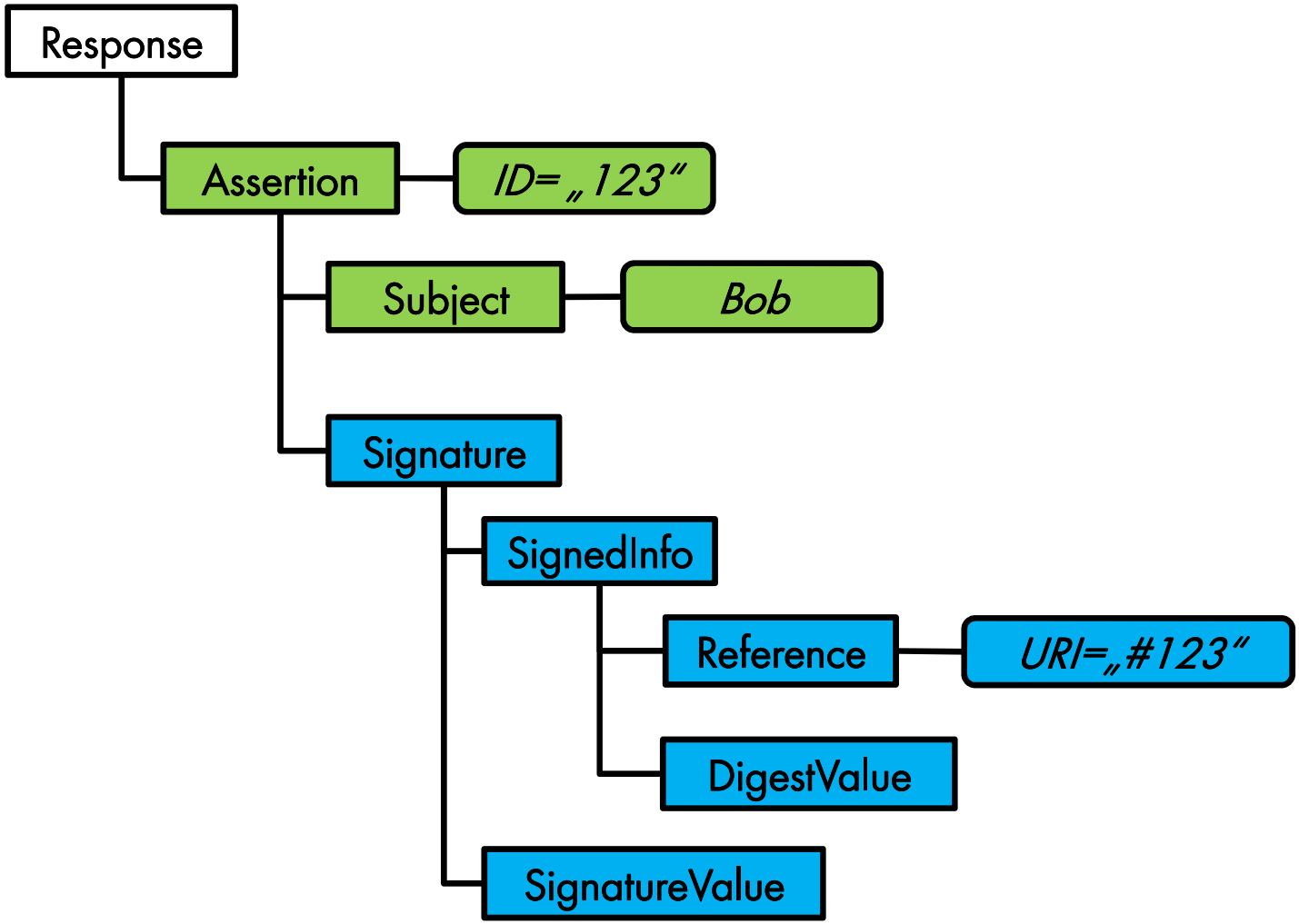
SAML Assertion

```
<saml:Assertion ID="123">
  <saml:Issuer>www.SecureIdP.com</saml:Issuer>
  <saml:Subject>
    <saml:NameID>Bob@SecureIdP.com</saml:NameID>
  </saml:Subject>
  <ds:Signature>...</ds:Signature>
  <saml:Conditions NotBefore="2011-08-08T14:42:00Z"
       NotOnOrAfter="2011-08-08T14:47:00Z">
    <saml:AudienceRestriction>
      <saml:Audience>www.SecureSP.com</saml:Audience>
    </saml:AudienceRestriction>
  </saml:Conditions>
</saml:Assertion>
```

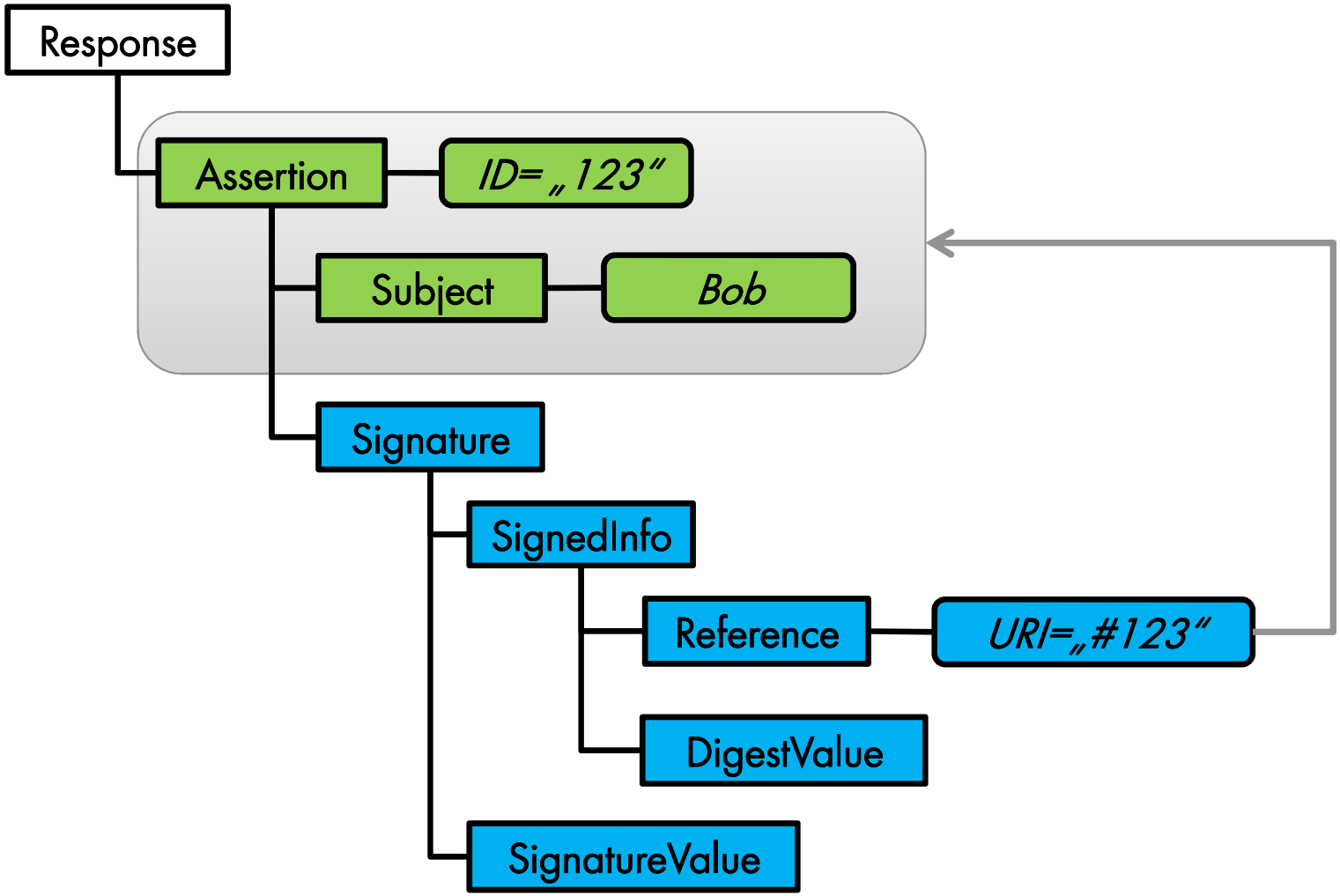
XML Signature

- Schützt die SAML Assertion selbst
- XML Signature gewährleistet
  - Datenintegrität und Unveränderbarkeit
  - Nichtwiderlegbarkeit (eindeutige Urheberschaft)
- Flexibel aber sehr komplex

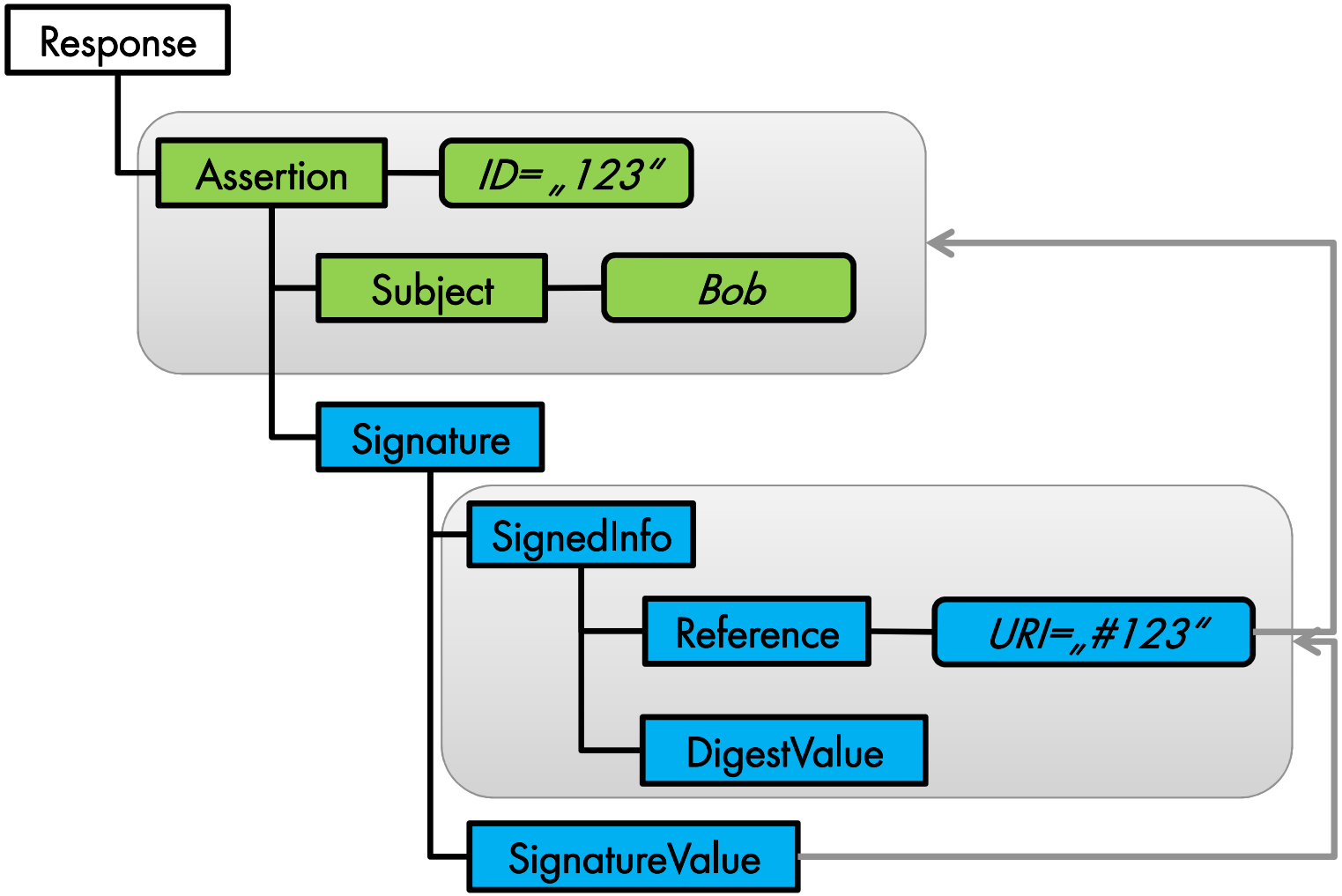
Schutz der Assertion mit XML Signature



Schutz der Assertion mit XML Signature



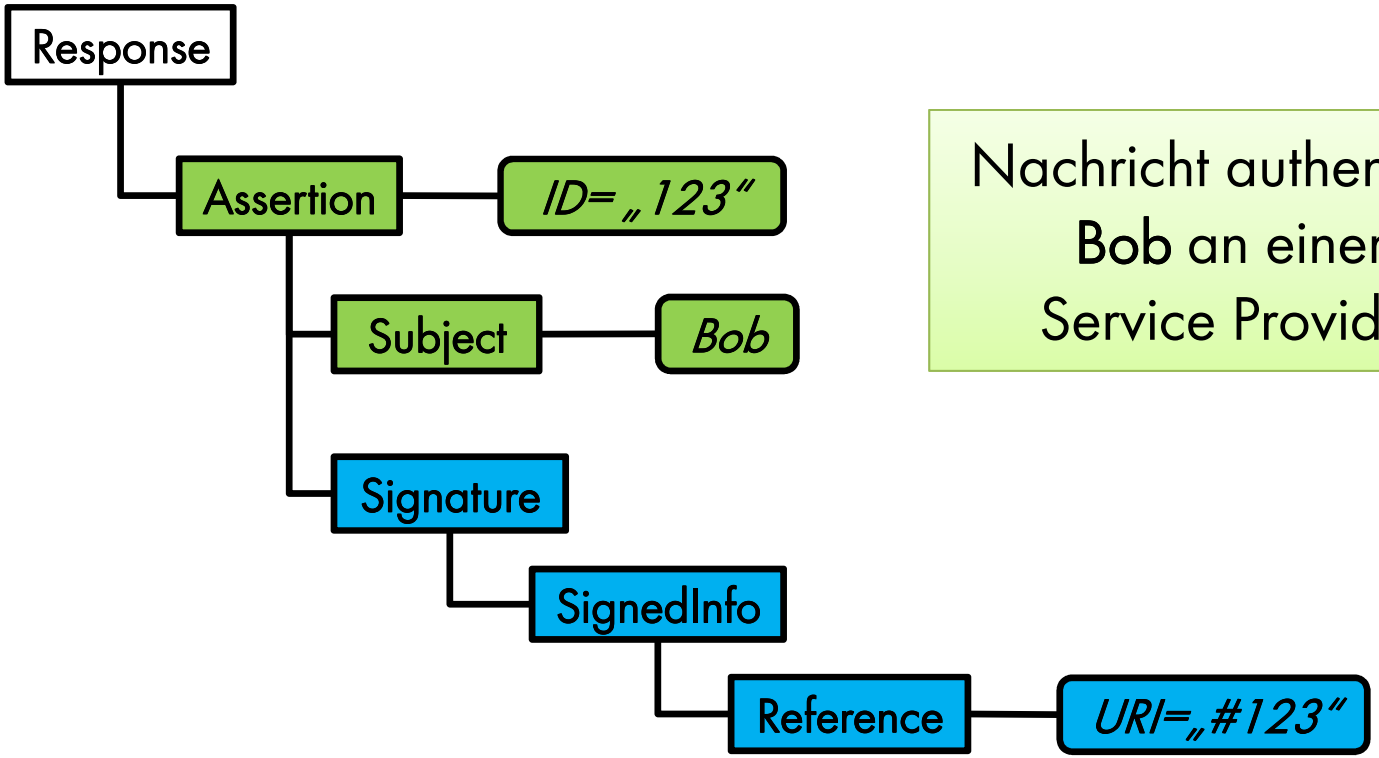
Schutz der Assertion mit XML Signature



XML Signature Wrapping Angriff

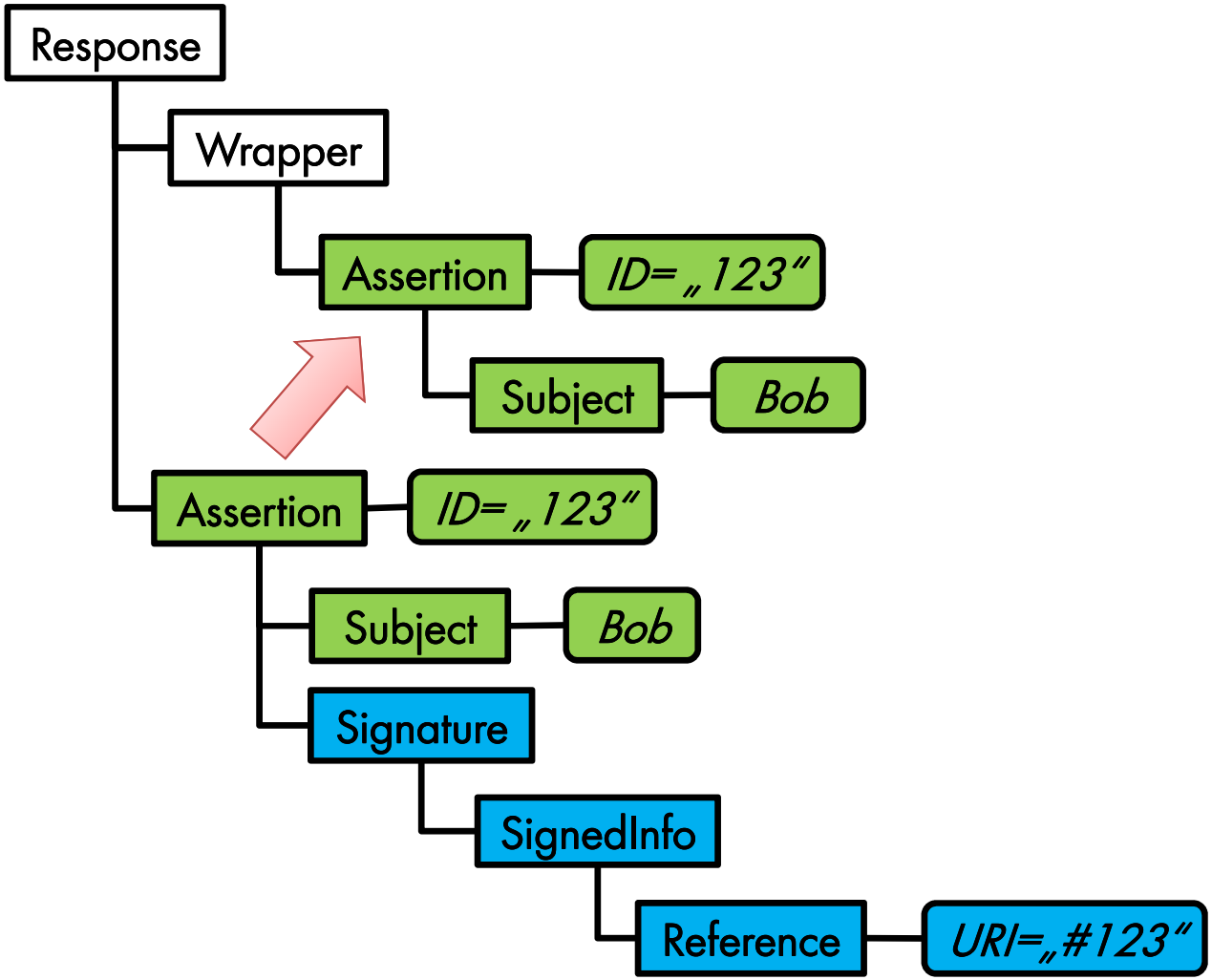
- Entdeckt von McIntosh und Austel in 2005
- Wirkung →Vollständige Aushebelung aller XML Signature Sicherheitsfunktionen
- Voraussetzung → Angreifer benötigt eine signierte Assertion:
  - Registrierter Benutzer bei Identity Provider
  - Google Hacking (z.B. in Supportforen usw.)
  - Bei Angriff erbeutet (z.B. per XSS, Malware ...)

Standard XML Signature Wrapping



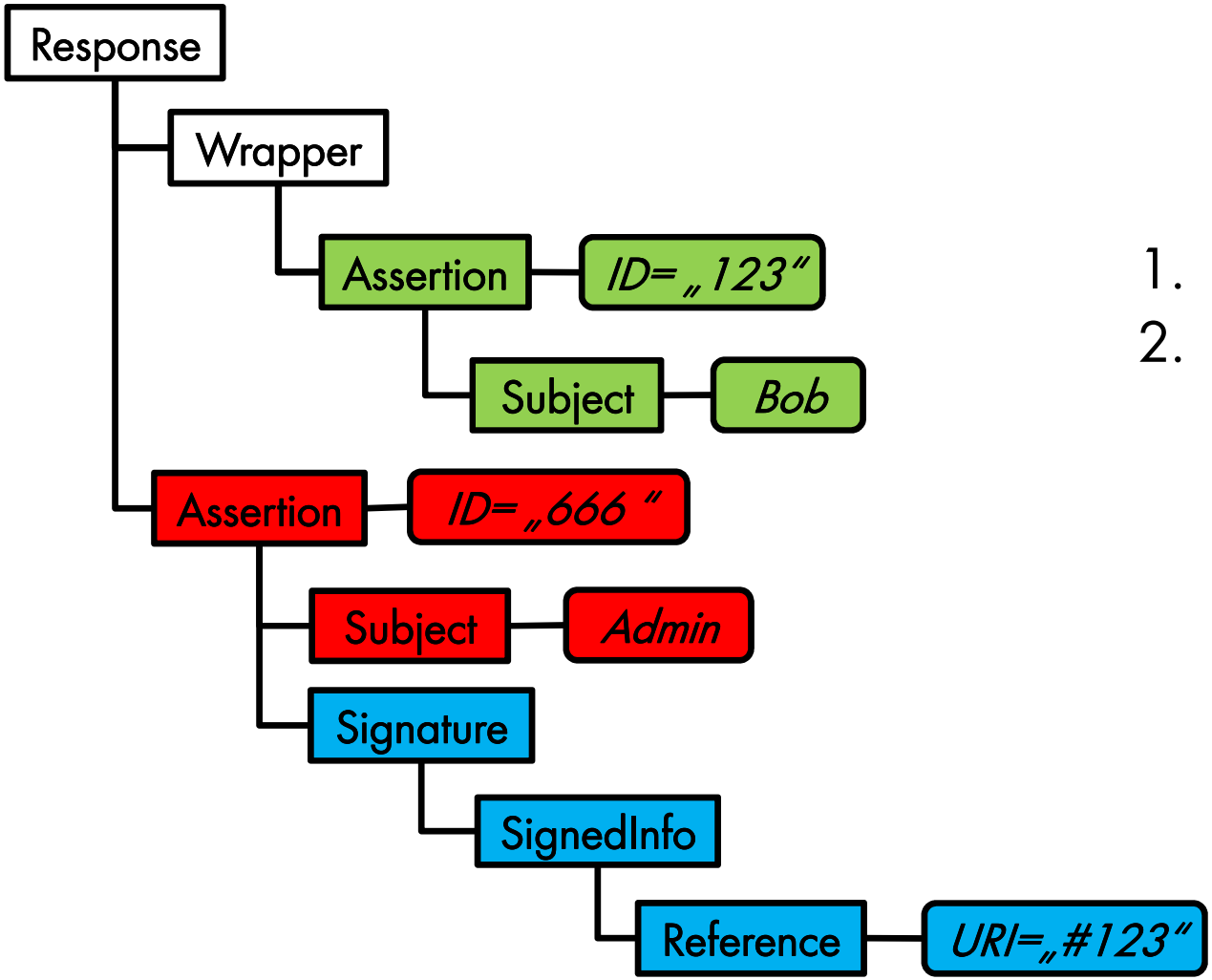
Nachricht authentisiert **Bob** an einem Service Provider.

Standard XML Signature Wrapping



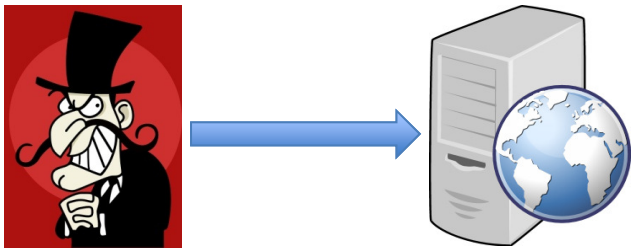
1. Assertion kopieren

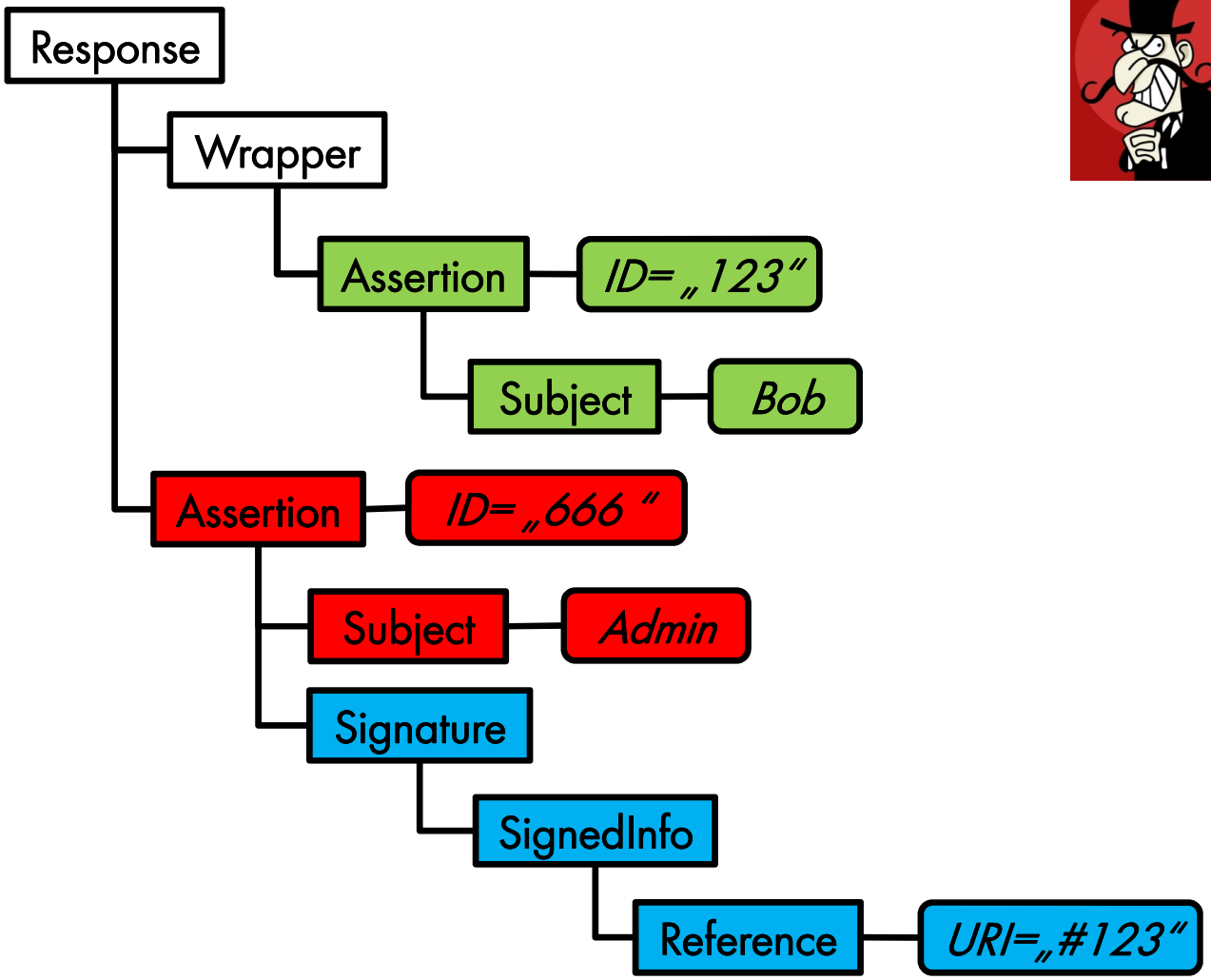
Standard XML Signature Wrapping



1. Assertion kopieren
2. Assertion modifizieren

Verarbeitung am Service Provider





Verarbeitung am Service Provider

Service Provider

Signatur validieren

- Response
  - Wrapper
    - Assertion — *ID=„123“*
      - Subject — *Bob*
  - Assertion — *ID=„666 “*
    - Subject — *Admin*
    - Signature
      - SignedInfo
        - Reference — *URI=„#123“*

Verarbeitung am Service Provider

Service Provider

Signatur validieren

Assertion verarbeiten

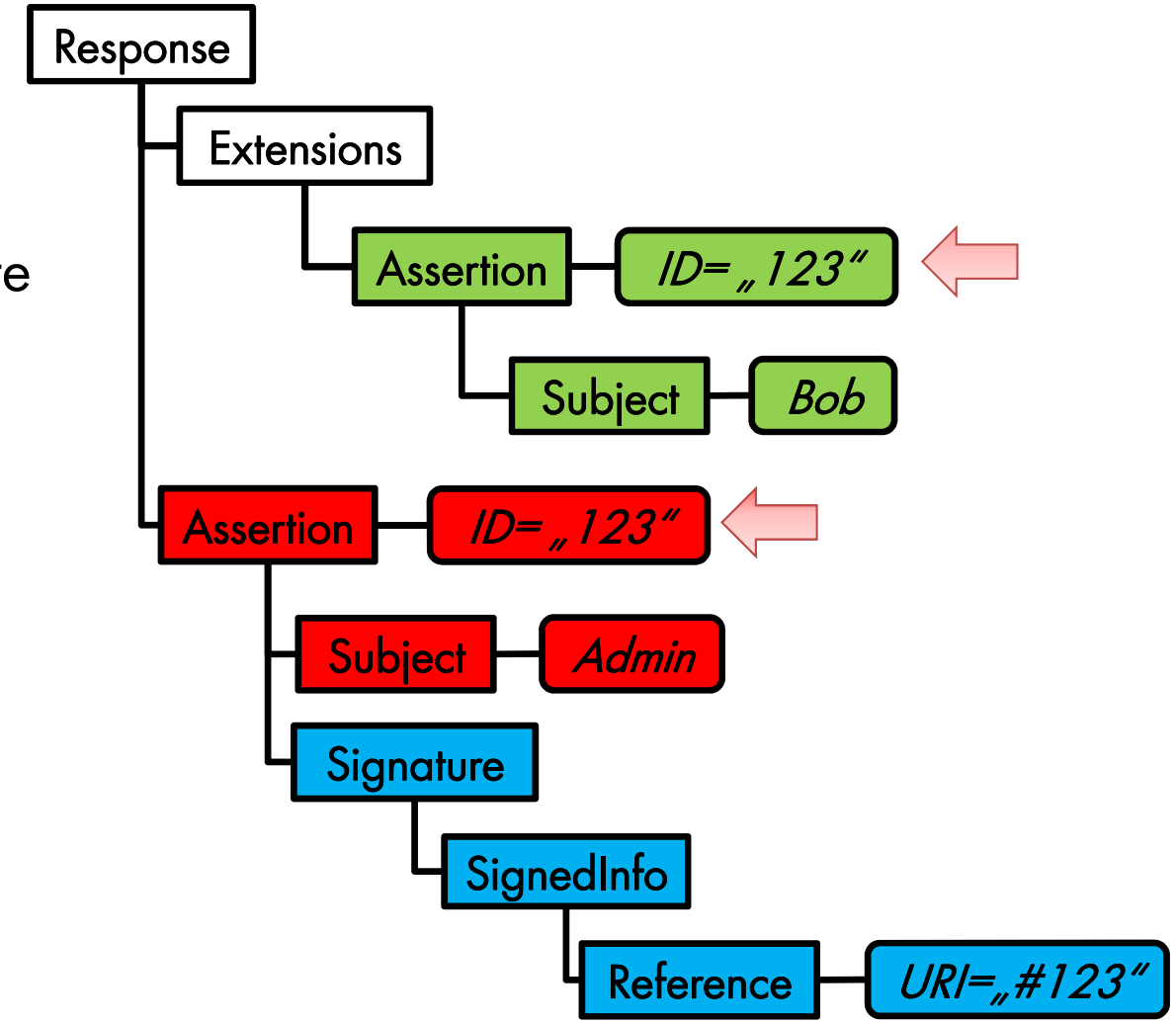
Angriff auf Shibboleth

- Implementiert Schutzmaßnahmen → Standardangriff nicht möglich
  - XML Schema-Validierung
    Verhindert vollkommen freies Einfügen von kopierten Assertions
  - Nur Enveloped Signatures erlaubt
    Knoten der XML Signature muss direkt in Assertion liegen
  - Gleichheit ID-Attribut
    Stringvergleich von ID-Attribut der signierten Assertion mit der Reference URI aus XML Signature

Shibboleth

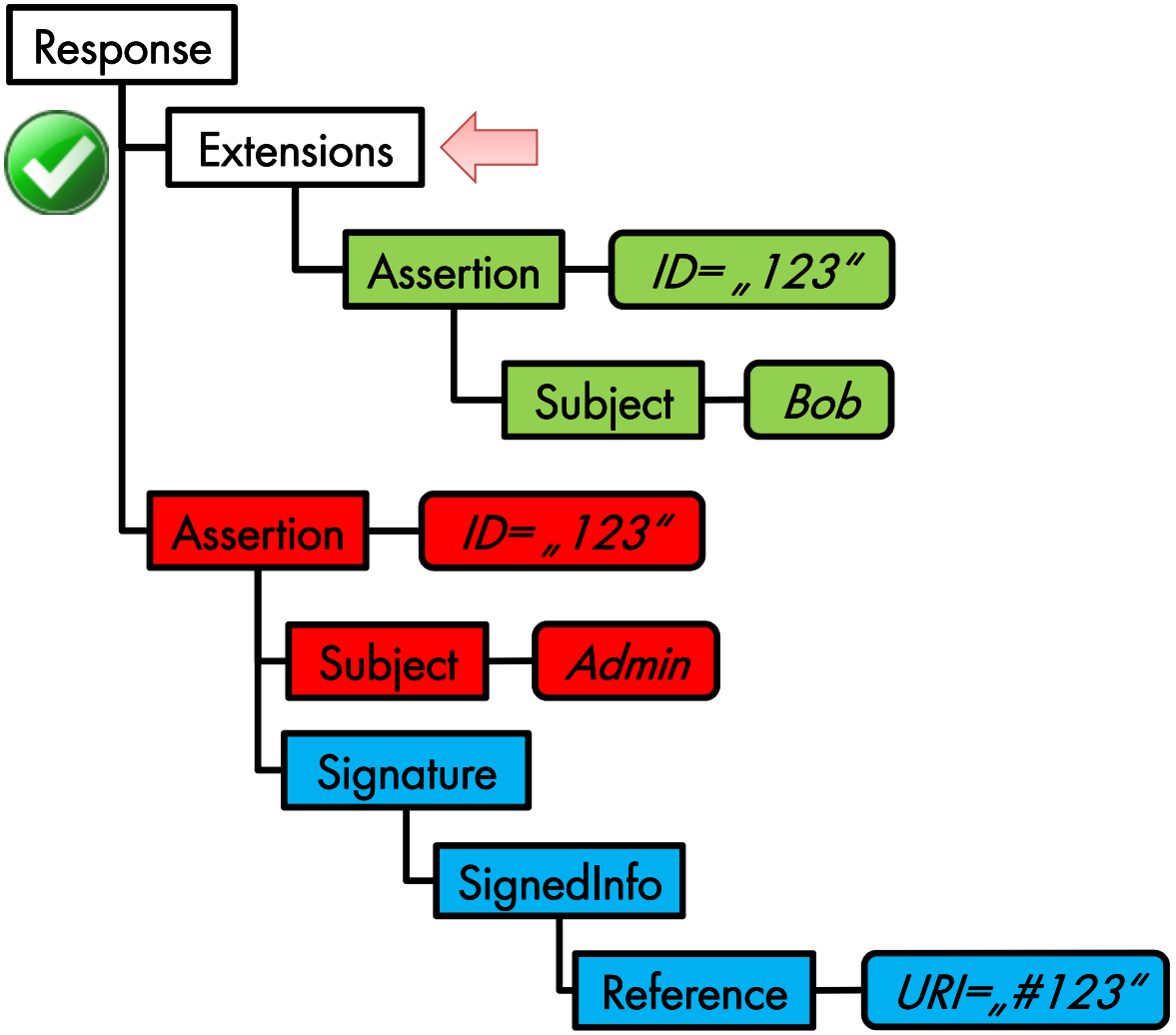
Neue XML Signature Wrapping Angriffsvariante

- Grundlegende Idee:
  Identische ID-Attribute



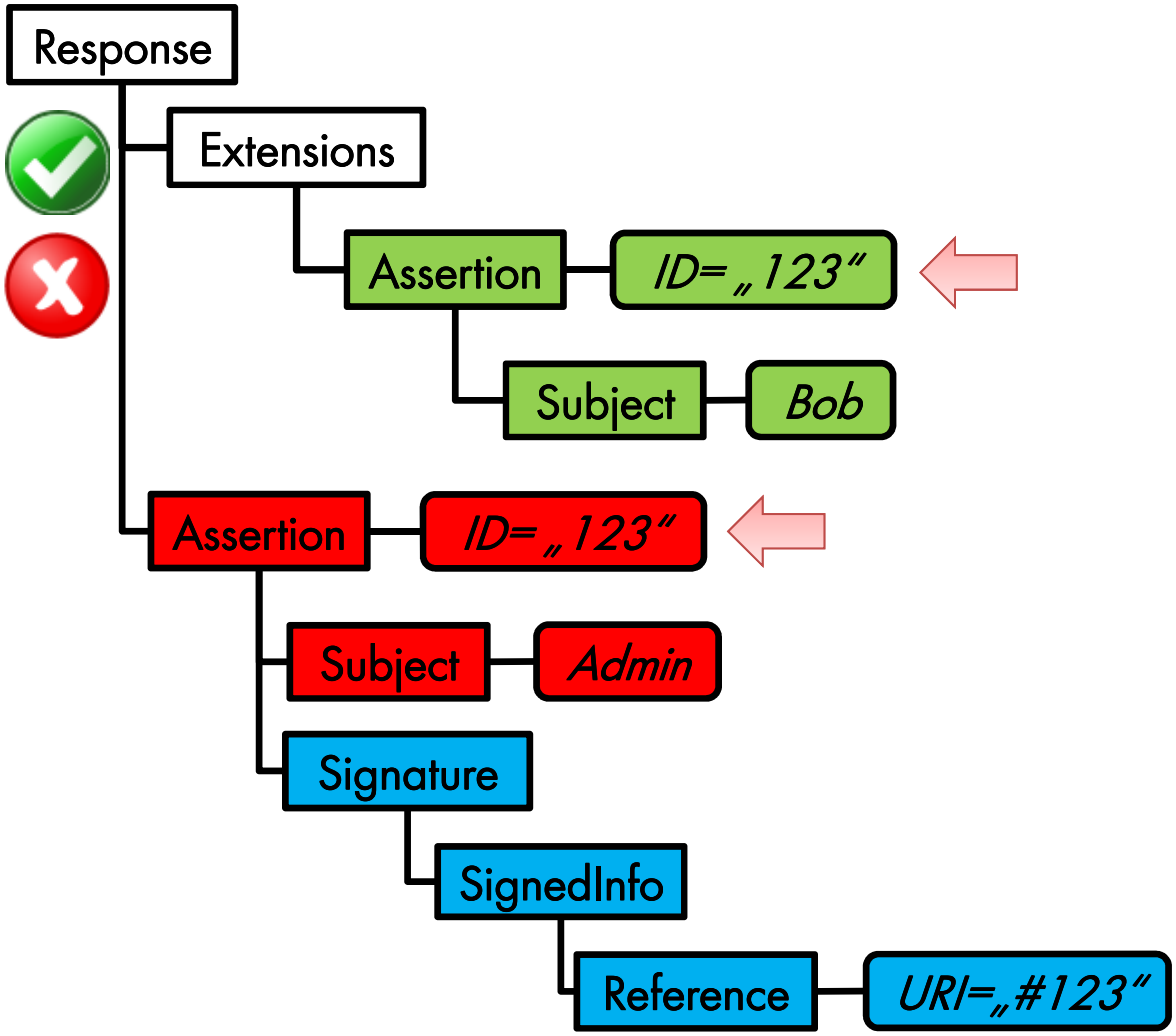
Verarbeitung beim Shibboleth Service Provider

1. Schema Validierung
   a. <Extensions>



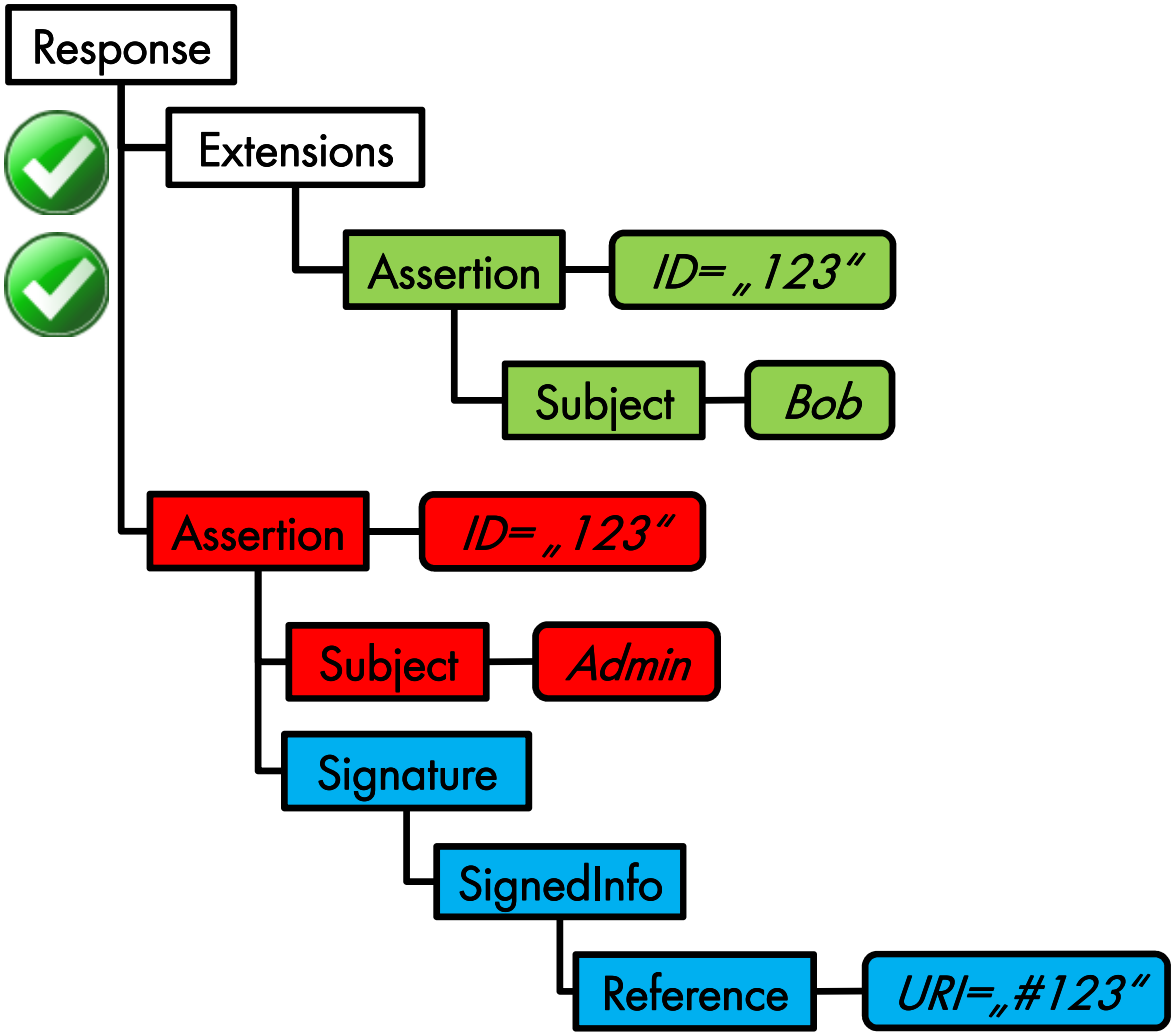
Verarbeitung beim Shibboleth Service Provider

1. Schema Validierung
   a. <Extensions>
   b. Doppeltes ID-Attribut



Verarbeitung beim Shibboleth Service Provider

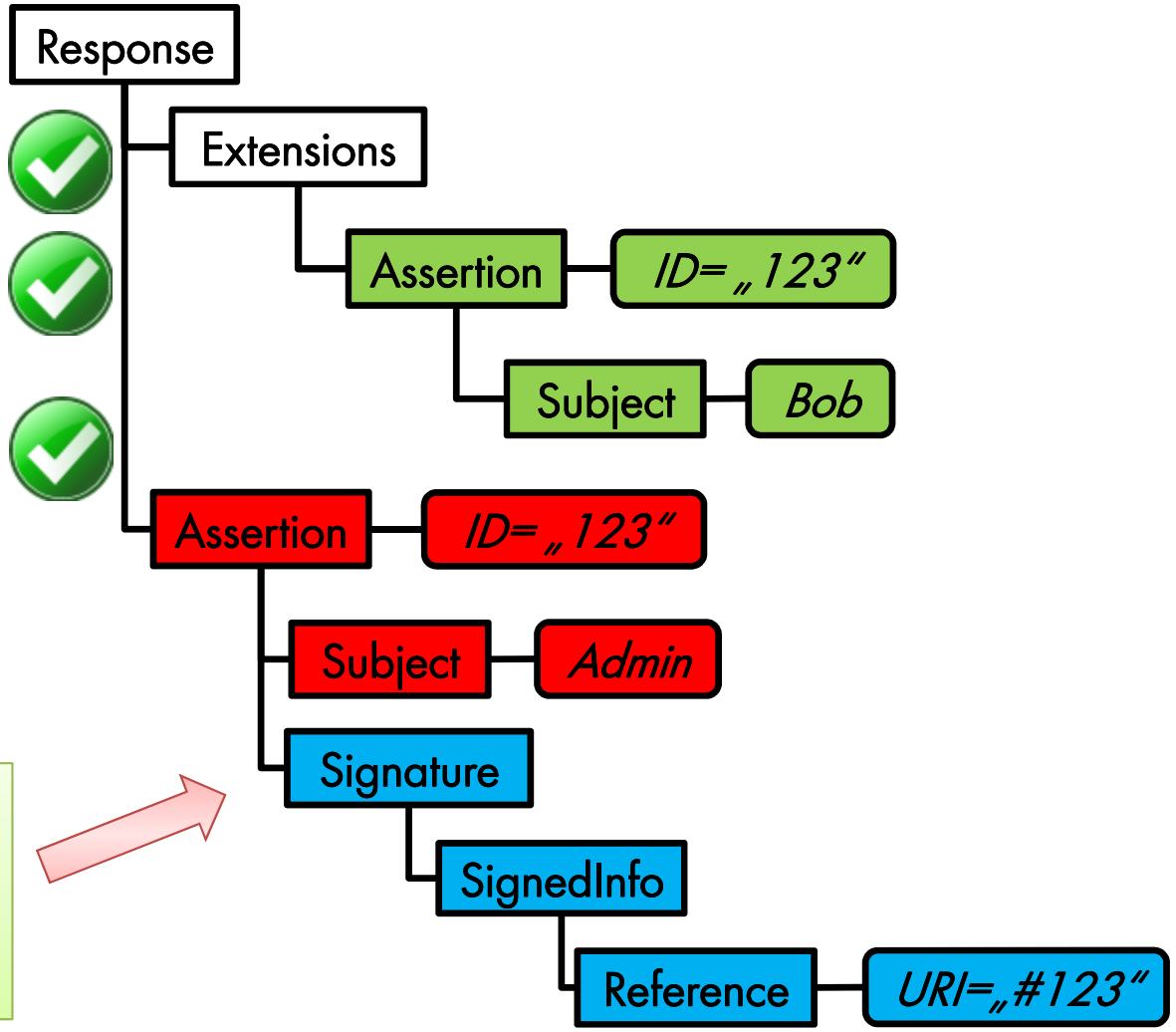
1. Schema Validierung
   a. <Extensions>
   b. Doppeltes ID-Attribut (Fehler in Xerces)



Verarbeitung beim Shibboleth Service Provider

1. Schema Validierung
   a. <Extensions>
   b. Doppeltes ID-Attribut (Fehler in Xerces)

2. Enveloped Signature
   a. Signatur in Assertion

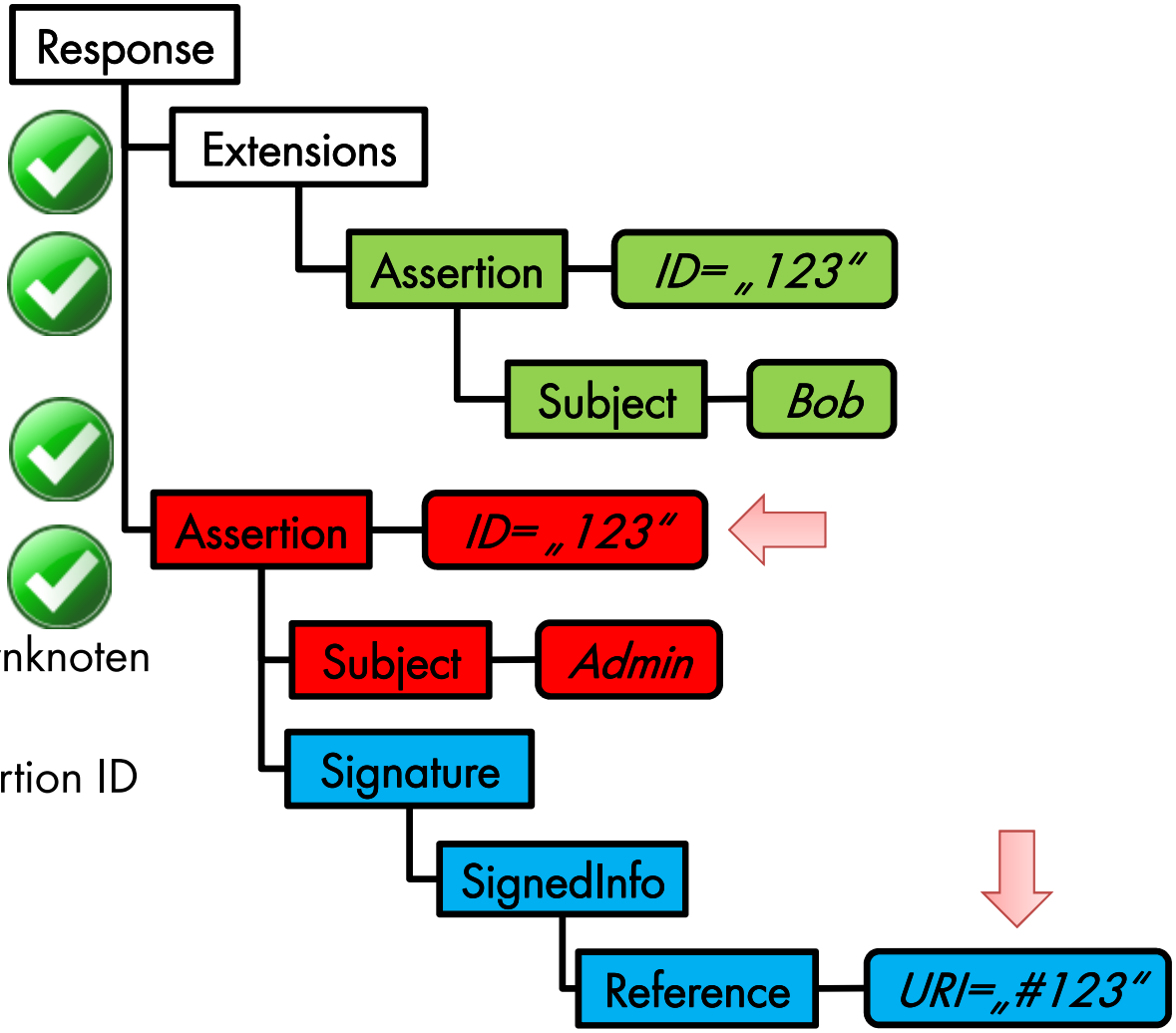


<Signature> ist Kind-Knoten von signierter Assertion

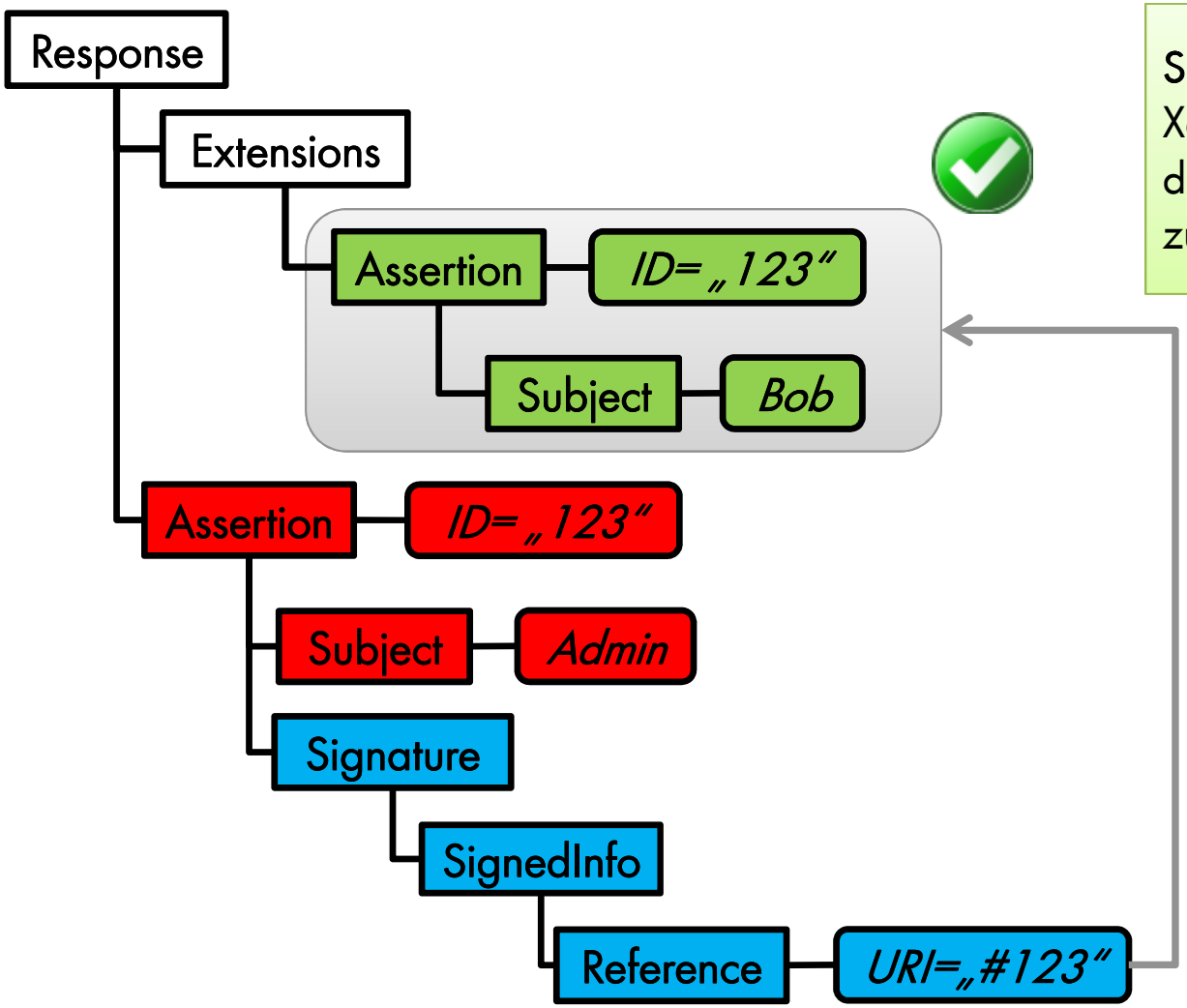
Verarbeitung beim Shibboleth Service Provider

1. Schema Validierung
   a. <Extensions>
   b. Doppeltes ID-Attribut (Fehler in Xerces)
2. Enveloped Signature
   a. Signatur in Assertion
3. Signature Reference
   a. Stringvergleich mit Elternknoten

   Reference URI $\overset{?}{==}$ Assertion ID

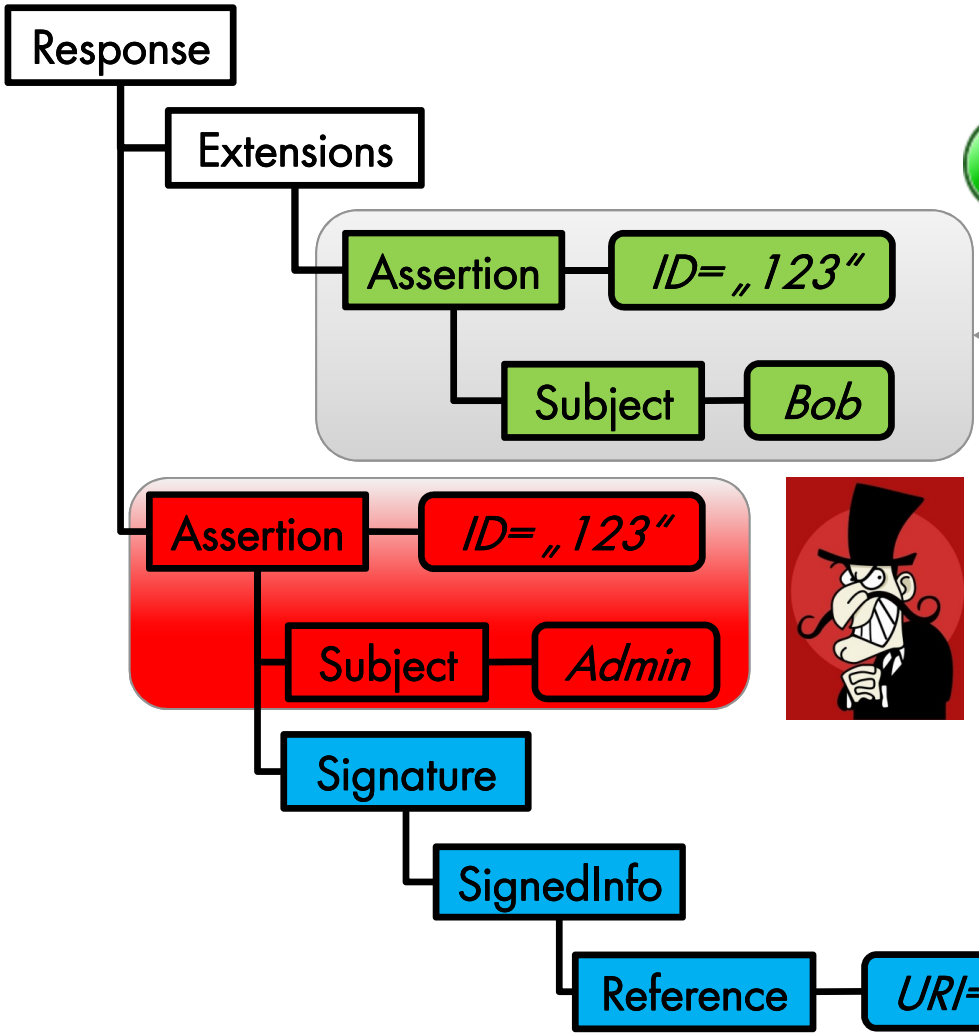


Verarbeitung beim Shibboleth Service Provider (C++ Implementierung)



Signaturverifikation
Xerces *getElementById()* liefert bei doppelten IDs **erstes** Element zurück (C++).

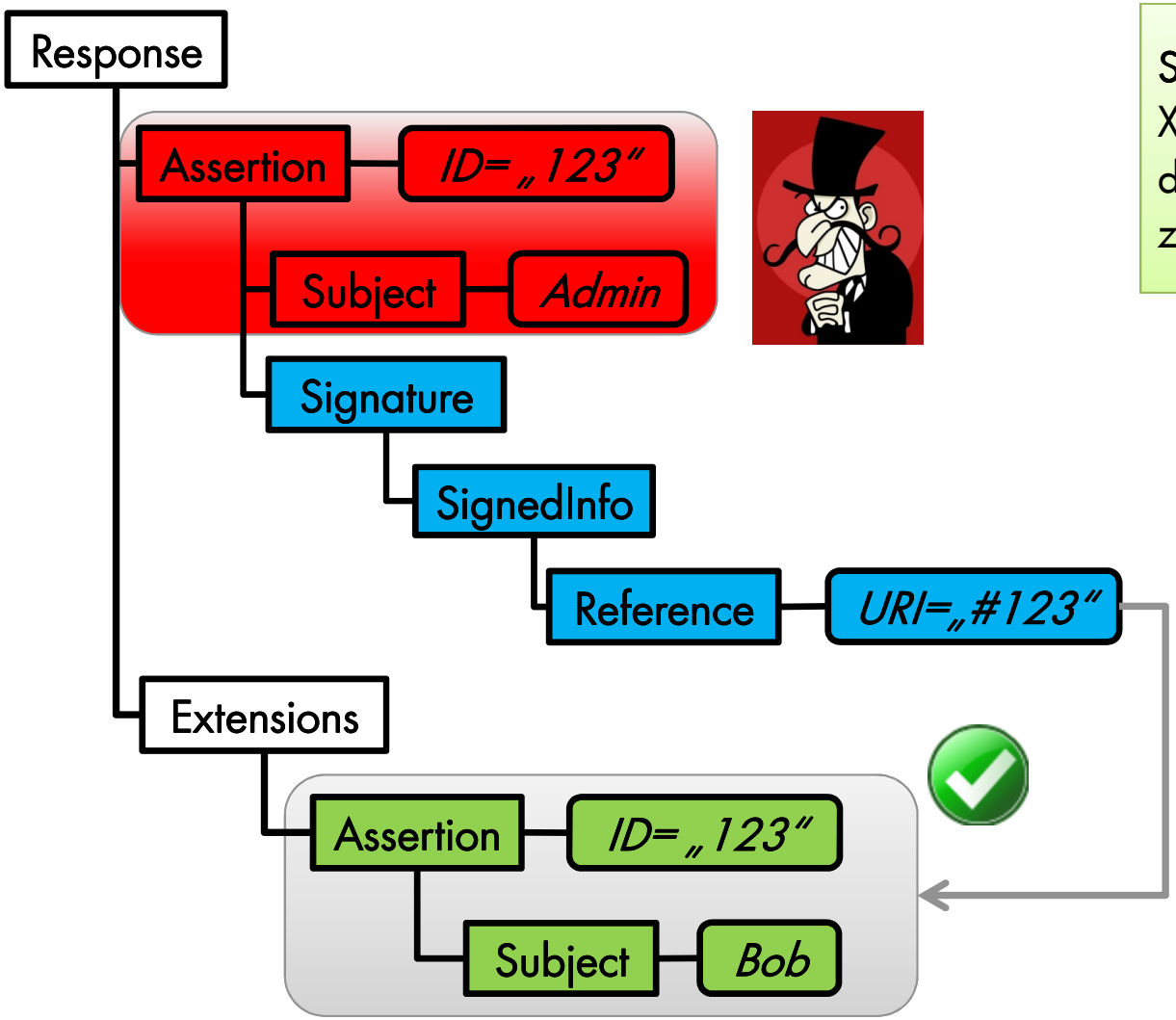
Verarbeitung beim Shibboleth Service Provider (C++ Implementierung)



Signaturverifikation
Xerces *getElementById()* liefert bei doppelten IDs **erstes** Element zurück (C++).

Assertion verarbeiten
Anwendungslogik verarbeitet Assertion aus <Response>.

Verarbeitung beim Shibboleth Service Provider (Java Implementierung)

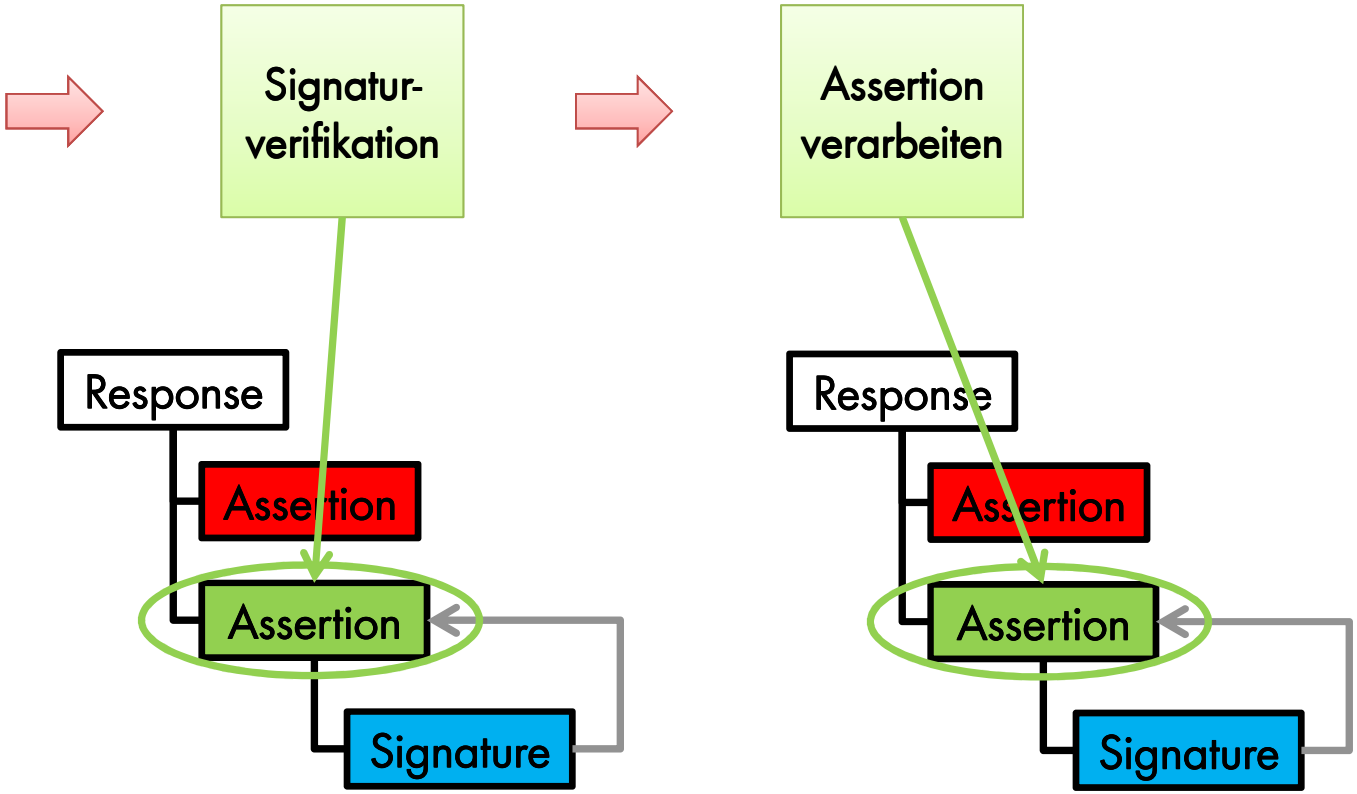


Signaturverifikation
Xerces *getElementById()* liefert bei doppelten IDs **letztes** Element zurück (Java).

Assertion verarbeiten
Anwendungslogik verarbeitet Assertion aus <Response>.

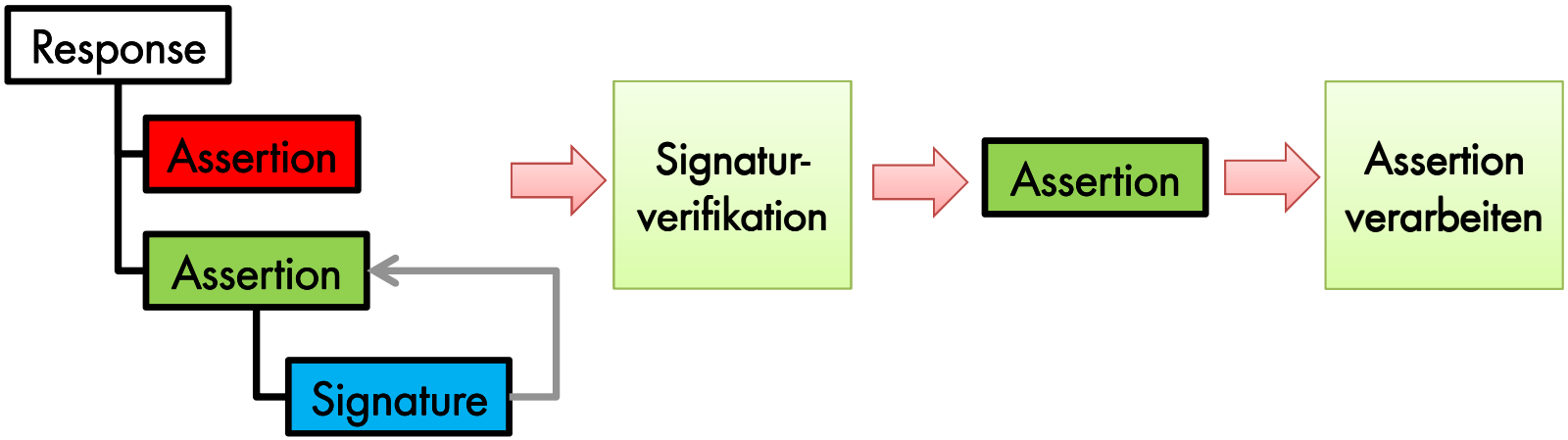
XML Signature Wrapping verhindern

- Jedes einzelne Verarbeitungsmodul muss die von der Signatur geschützten Daten verarbeiten.



Gegenmaßnahme I: Strict Filtering

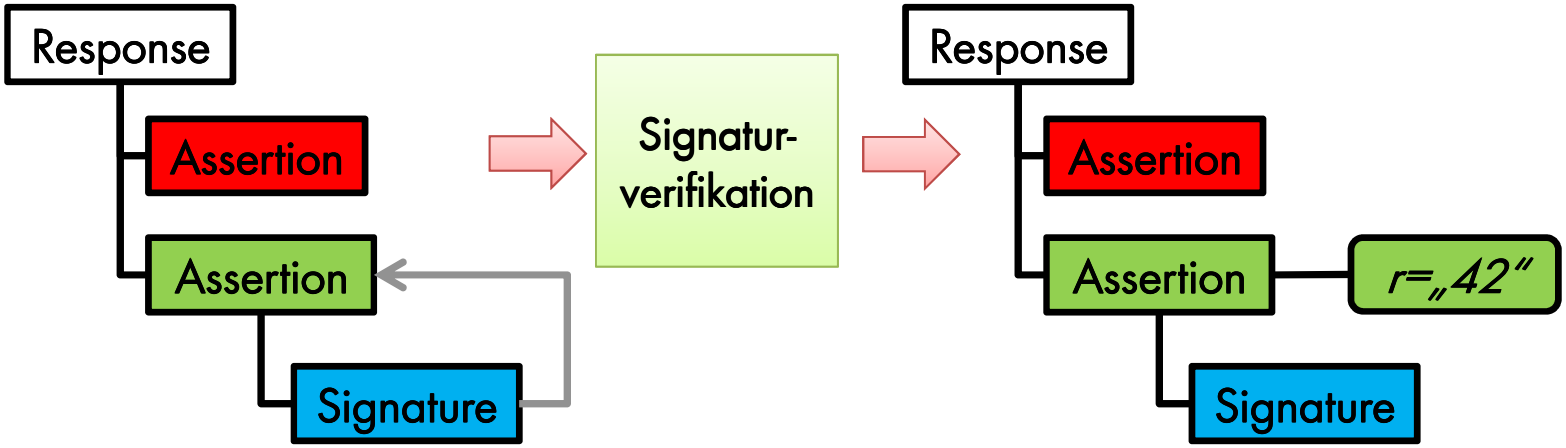
- Signaturverifikation gibt keinen Boolean-Wert zurück, sondern die signierte Assertion.



- Positiv:
  - Alle Module arbeiten mit gleichen Daten
- Negativ
  - Arbeiten mit (modifizierten) Teilbäumen
  - Nicht in verteilten SOA-Umgebungen einsetzbar (XML Security Gateway)

Gegenmaßnahme II: Geprüfte Elemente markieren

- Signaturverifikation markiert die signierten und geprüften Teile im XML-Dokument
  - Markierung mit Zufallszahl *r* (Weitergabe als Parameter)



  - Positiv:
    - Alle Module arbeiten auf einem Dokument
    - Auch in verteilten SOA-Umgebungen einsetzbar (XML Security Gateway)
  - Negativ:
    - Erfordert Erweiterung des SAML XML Schemas

Fazit

- Neue Klasse von XML Signature Wrapping Angriffen entdeckt
- Shibboleth trotz spezieller Sicherungsmaßnahmen anfällig (CVE-2011-1411)
  - Schwachstellen gefixt (SP ab Version 2.4.3; IdP ab Version 2.3.2)
- XML Signature Wrapping sind seit 2005 bekannt, aber
  - weit verbreitet
  - schwer zu verhindern (viele Permutationen, Bugs in verwendeten Libraries)
  - bisher nicht im Fokus der Forschung
- Bei Einsatz von XML Signature immer Schutzmaßnahmen einbauen!

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?

Andreas Mayer
andreas.mayer@wuerth.com