BitFlip: Determine a Data's Signature Coverage from within the Application

Henrich C. Pöhls
Institute of IT-Security and Security Law
University of Passau, Germany
hp@sec.uni-passau.de
+498515093217

OWASP
23.06.2010

The OWASP Foundation
http://www.owasp.org

me, myself and this talk

- M.Sc. Information Security from Royal Holloway
- Diplom Informatik from University of Hamburg
- currently PhD student at University of Passau

ReSCUe IT

SPONSORED BY THE

Federal Ministry
of Education
and Research

ReSCUe IT:

- General: IT supported robust & secure Supply Chains
- Our Goal: Legally compliant & manageable integrity and authenticity statements for the data

Outline

- Problem & Motivation
- BitFlip Approach
- What BitFlip is not ...
- What BitFlip can do ... example XML-wrapping
- Conclusion

Problem: Message Security Layer vs. Application Layer

Design is layered

- Application Layer
  - Application logic works on data
- Data comes in by message
  - Application extracts data from message
- Security layer protects message (or part thereof)
  - Signed messages are verified before given to app.

Layered Security:

interlinking between layers must stay “in-sync”

Example: XML SOAP message security

Available security mechanism for SOAP messages:

- WS-Security (Tokens ...)
- XML Signature (and Encryption)

Security checks considered “good practice”:

- well defined XML schema
- rigorous schema validation
- validity check of signing public-key
- enforce strict security policies

Example: XML SOAP message security

Available security mechanism for SOAP messages:

- WS-Security (Tokens ...)
- XML Signature (and Encryption)

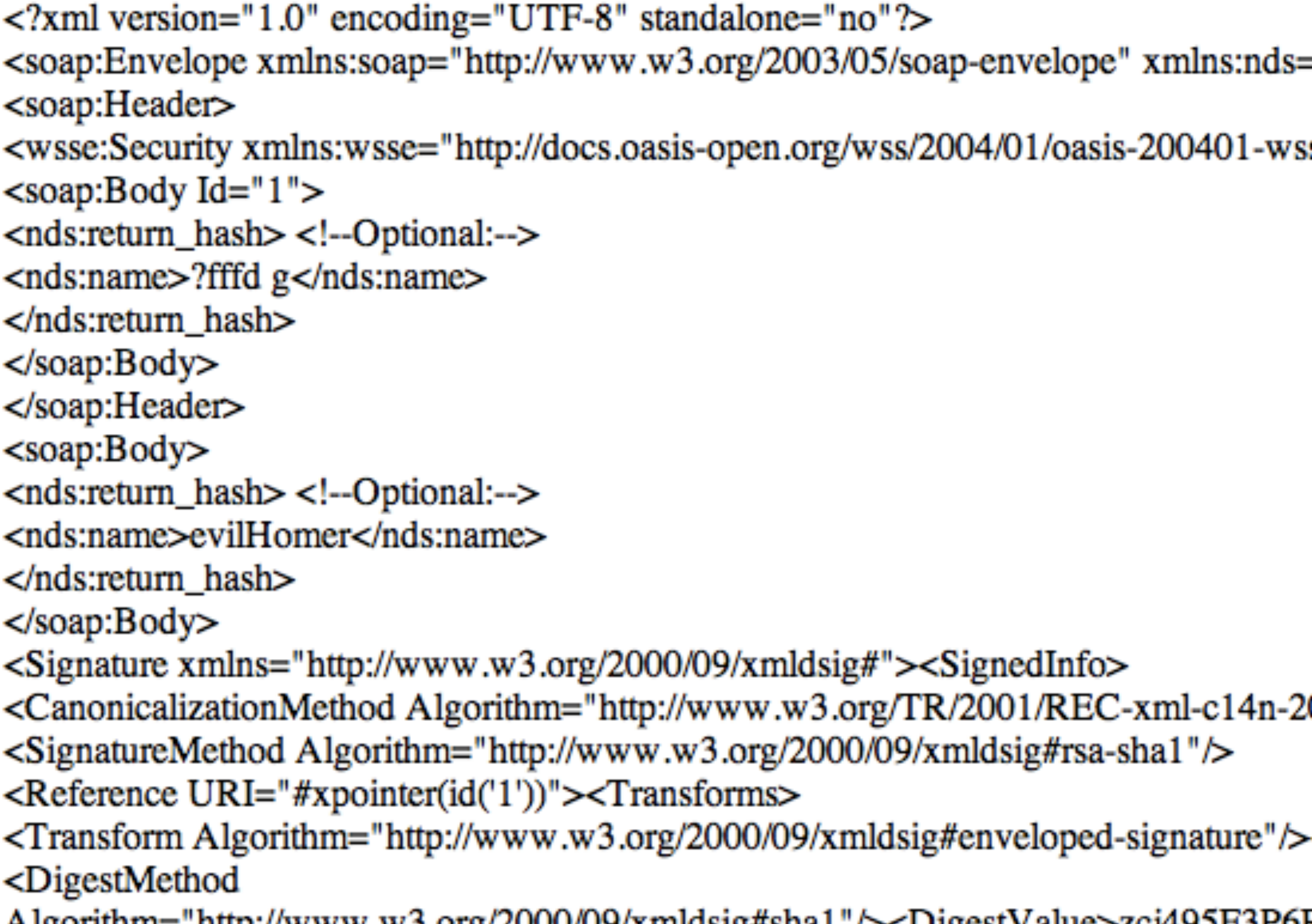
Security checks considered “good practice”:

- well defined XML schema
- rigorous schema validation
- validity check of signing public-key
- enforce strict security policies

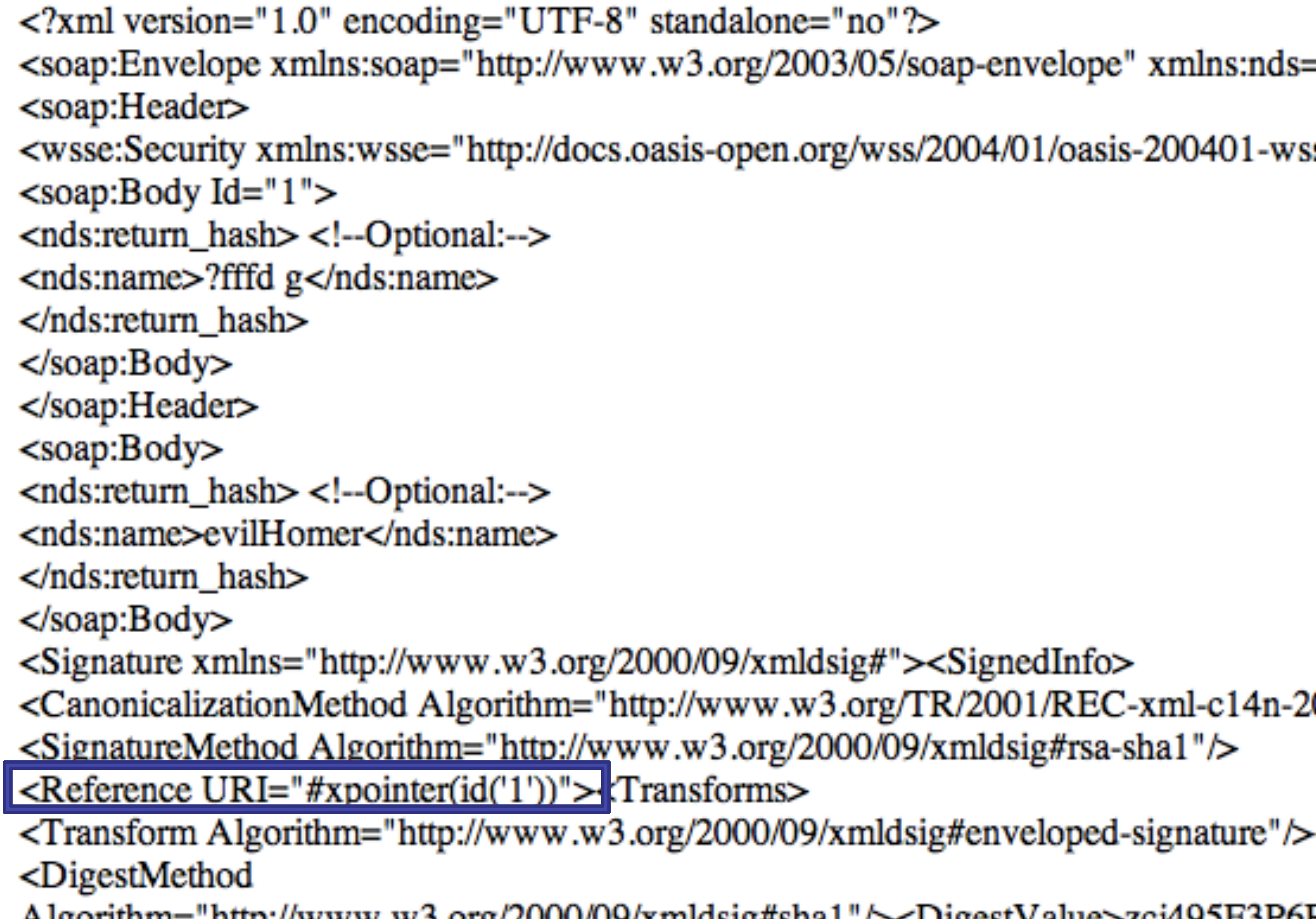
... but attacks on real world web services happen.

Authenticate not just the message,
but everything that is used to determine
the meaning of the message.

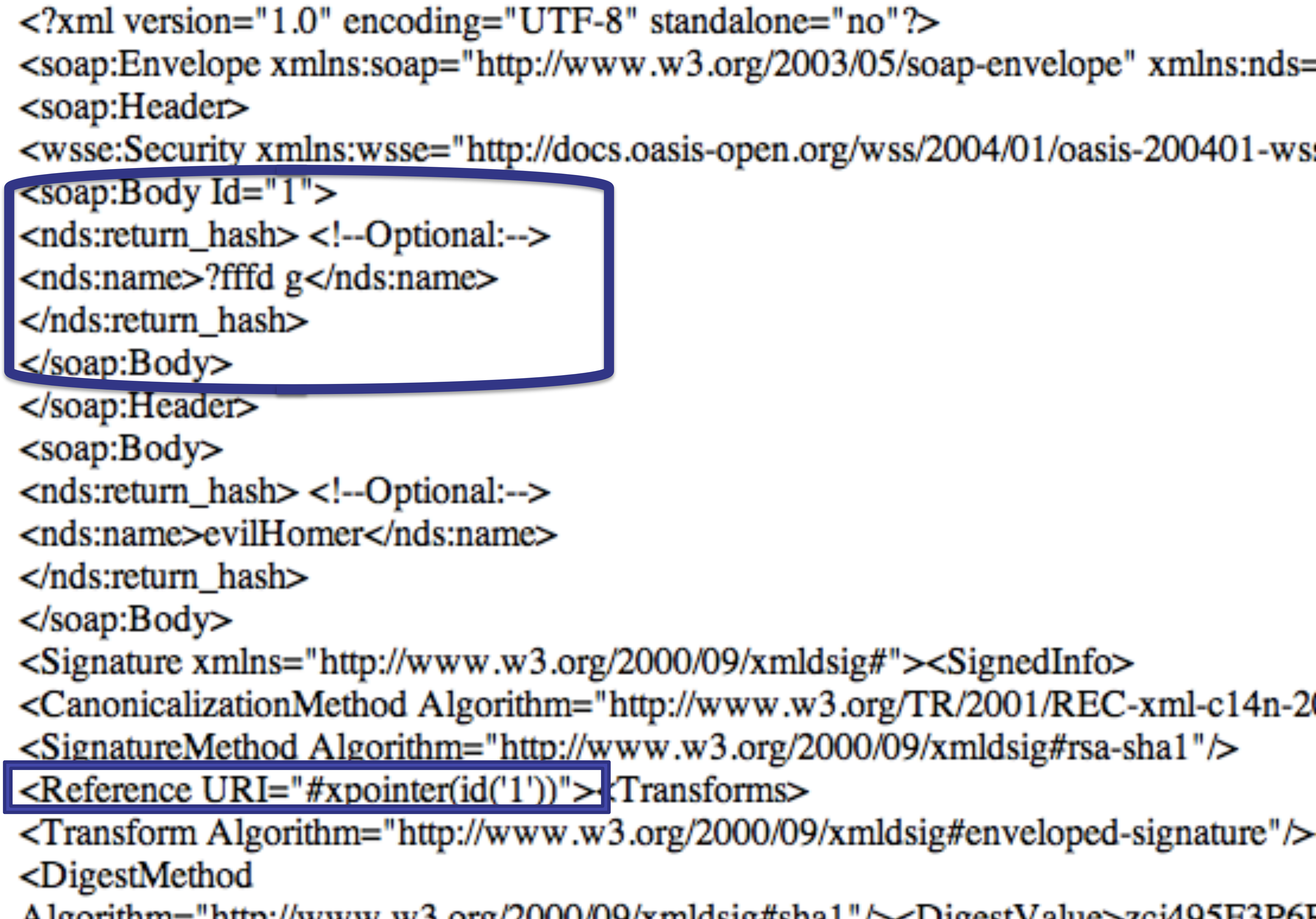
Ferguson and Schneier



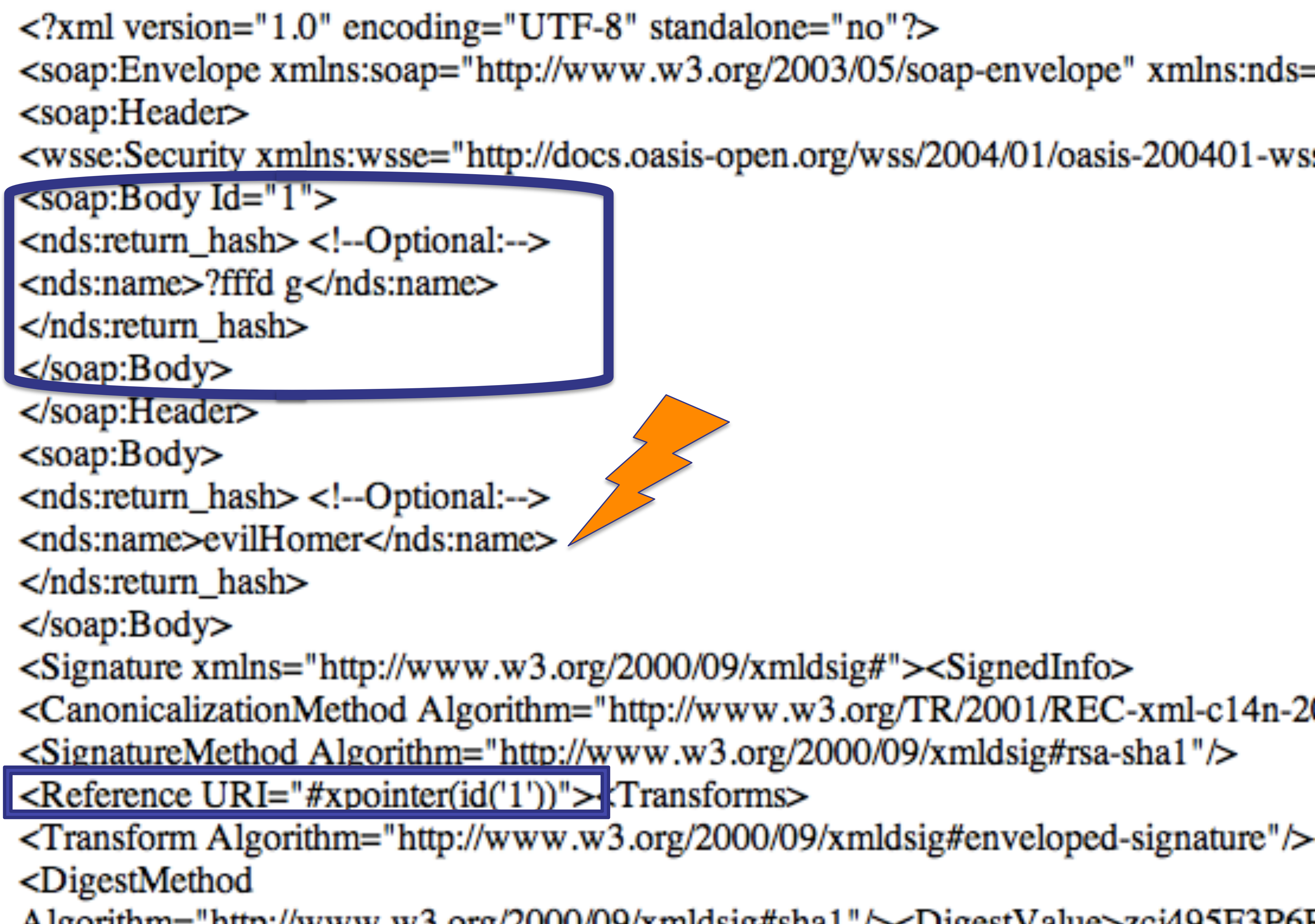
```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds=
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-ws
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nds:name>?fffd g</nds:name>
</nds:return_hash>
</soap:Body>
</soap:Header>
<soap:Body>
<nds:return_hash> <!--Optional:-->
<nds:name>evilHomer</nds:name>
</nds:return_hash>
</soap:Body>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-2
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<Reference URI="#xpointer(id('1'))"><Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zci495F3P6
```



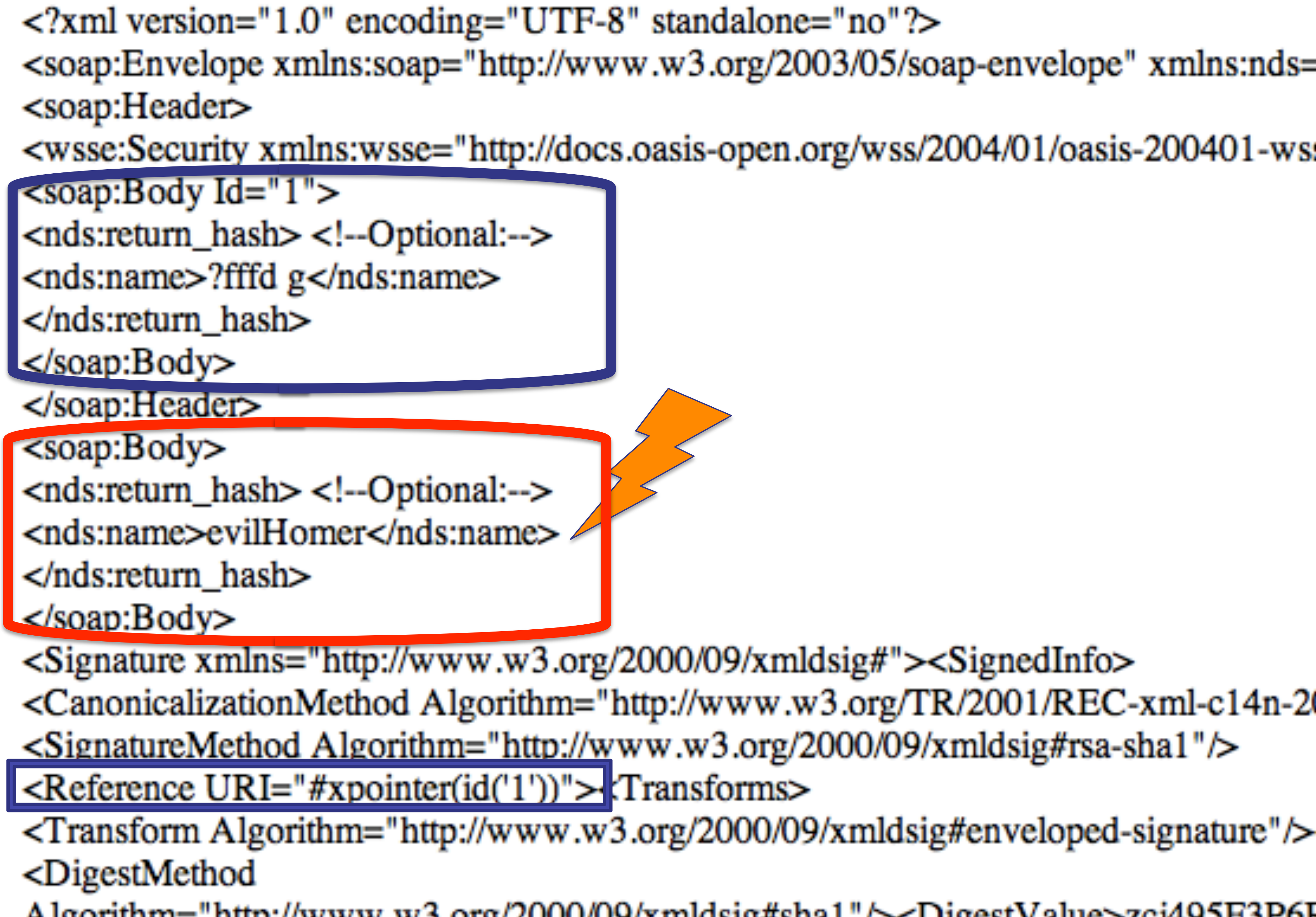
```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds=
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nds:name>?fffd g</nds:name>
</nds:return_hash>
</soap:Body>
</soap:Header>
<soap:Body>
<nds:return_hash> <!--Optional:-->
<nds:name>evilHomer</nds:name>
</nds:return_hash>
</soap:Body>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-2
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<Reference URI="#xpointer(id('1'))"><Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zqi495F3P6
```



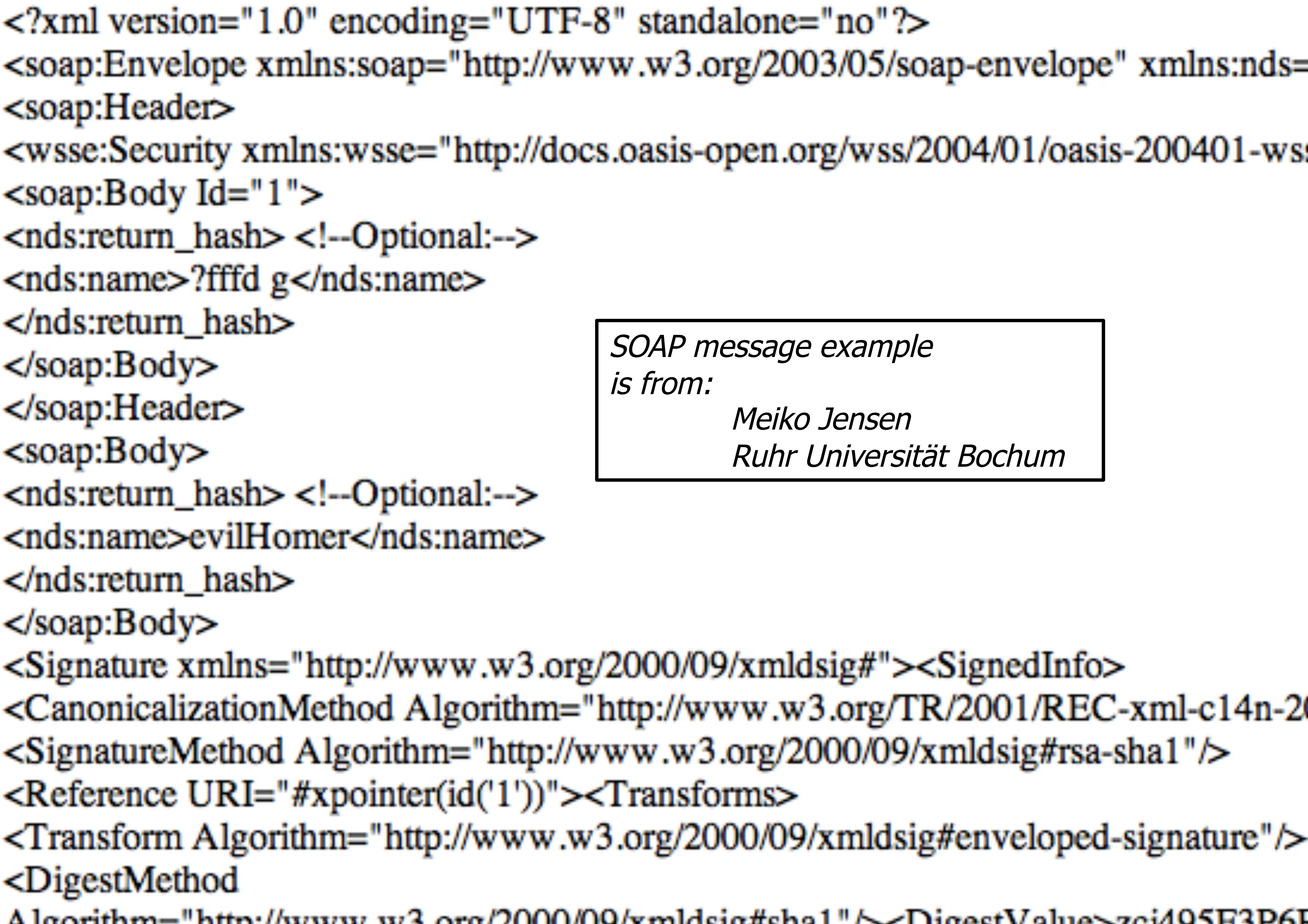
```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds=
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nds:name>?fffd g</nds:name>
</nds:return_hash>
</soap:Body>
</soap:Header>
<soap:Body>
<nds:return_hash> <!--Optional:-->
<nds:name>evilHomer</nds:name>
</nds:return_hash>
</soap:Body>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<Reference URI="#xpointer(id('1'))"><Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zoi495F3P6
```



```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds=
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-ws
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nds:name>?fffd g</nds:name>
</nds:return_hash>
</soap:Body>
</soap:Header>
<soap:Body>
<nds:return_hash> <!--Optional:-->
<nds:name>evilHomer</nds:name>
</nds:return_hash>
</soap:Body>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-2
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<Reference URI="#xpointer(id('1'))"><Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6
```



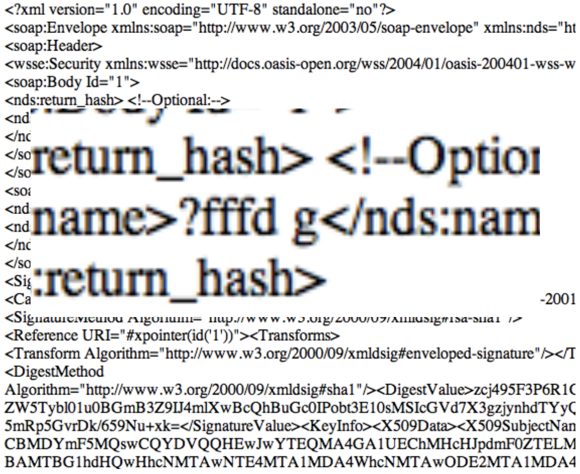
```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds=
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-ws
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nds:name>?fffd g</nds:name>
</nds:return_hash>
</soap:Body>
</soap:Header>
<soap:Body>
<nds:return_hash> <!--Optional:-->
<nds:name>evilHomer</nds:name>
</nds:return_hash>
</soap:Body>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-2
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<Reference URI="#xpointer(id('1'))"><Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zci495F3P6
```



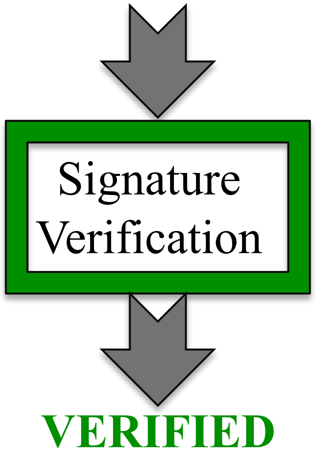
```xml
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds=
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-ws
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nds:name>?fffd g</nds:name>
</nds:return_hash>
</soap:Body>
</soap:Header>
<soap:Body>
<nds:return_hash> <!--Optional:-->
<nds:name>evilHomer</nds:name>
</nds:return_hash>
</soap:Body>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-2
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<Reference URI="#xpointer(id('1'))"><Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zei495F3P6
```

SOAP message example is from:
Meiko Jensen
Ruhr Universität Bochum

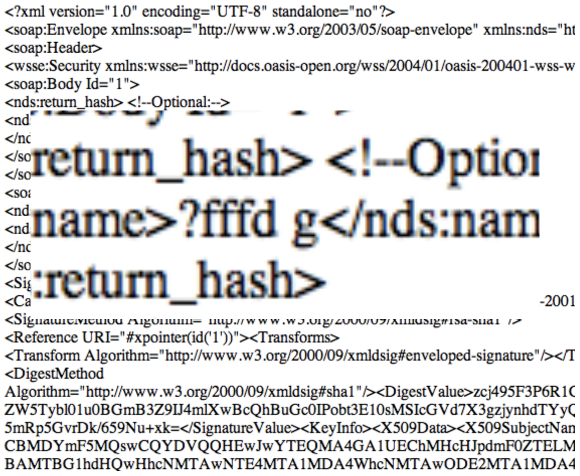
BitFlip: Observing the Signature Verification Outcome on Application Induced Errors



```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nd
</nc
</so  return_hash> <!--Optior
</so
<soa
<nd   name>?fffd g</nds:nam
<nd
</nc
</so
<Sig  :return_hash>
<Ca                                                                            -2001
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<Reference URI="#xpointer(id('1'))"><Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C
ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyQ
5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan
CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM
BAMTBG1hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4
```

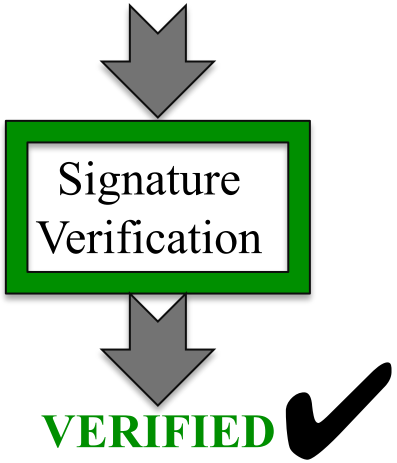


BitFlip: Observing the Signature Verification Outcome on Application Induced Errors



```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nd
</nc
</so
</so
<so
<nd
<nd
</nc
</so
<Si
<Ca                                                                          -2001
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<Reference URI="#xpointer(id('1'))"><Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C
ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyQ
5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan
CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM
BAMTBG1hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4
```

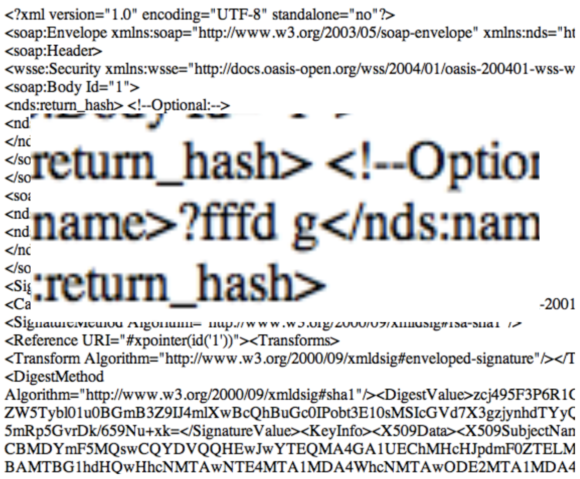
```
return_hash> <!--Optior
name>?fffd g</nds:nam
:return_hash>
```



Signature Verification

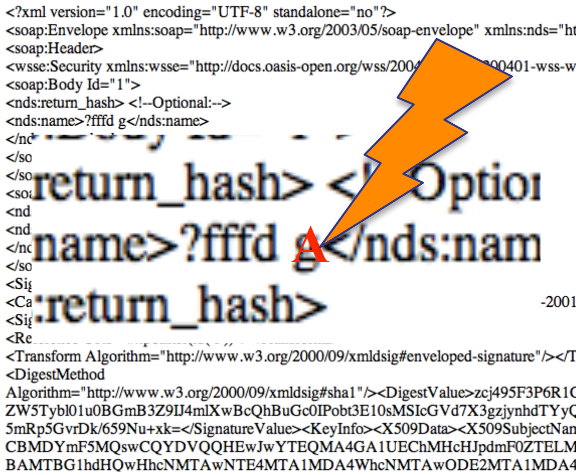
VERIFIED ✔

BitFlip: Observing the Signature Verification Outcome on Application Induced Errors



```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
return_hash> <!--Optio
name>?fffd g</nds:nam
:return_hash>
                                                                            -2001
<Reference URI="#xpointer(id('1'))"><Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C
ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC
5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan
CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM
BAMTBG1hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4
```

BitFlip: controlled change of single character

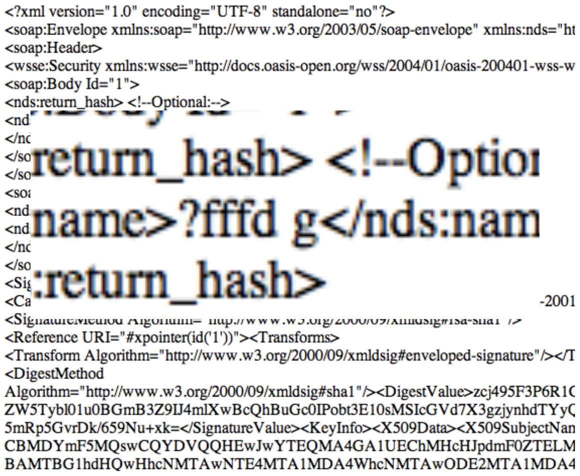


```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004          00401-wss-w
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nds:name>?fffd g</nds:name>
return_hash> <   Optio
name>?fffd A</nds:nam
:return_hash>
                                                                            -2001
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C
ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC
5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan
CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM
BAMTBG1hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4
```

Signature Verification

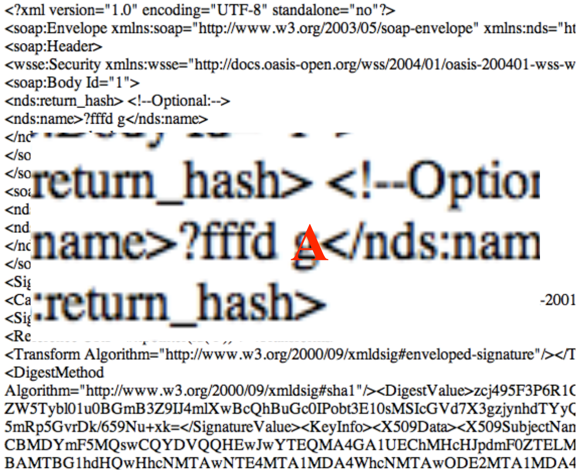
VERIFIED ✔

BitFlip: Observing the Signature Verification Outcome on Application Induced Errors



```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nd
</nc
</so  return_hash> <!--Optio
</so
<so
<nd   name>?fffd g</nds:nam
<nd
</nc
</so
<Si   :return_hash>
<Ca                                                                             -2001
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<Reference URI="#xpointer(id('1'))"><Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C
ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC
5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan
CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM
BAMTBG1hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4
```

BitFlip: controlled change of single character



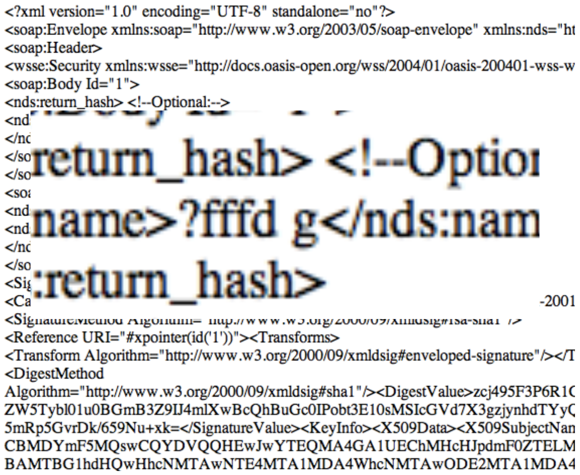
```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nds:name>?fffd g</nds:name>
</nc
</so
</so  return_hash> <!--Optio
<so
<nd
<nd   name>?fffd A</nds:nam
</nc
</so
<Si
<Ca   :return_hash>                                                             -2001
<Si
<Re
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C
ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC
5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan
CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM
BAMTBG1hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4
```

Signature Verification

VERIFIED ✔

Signature Verification

BitFlip: Observing the Signature Verification Outcome on Application Induced Errors

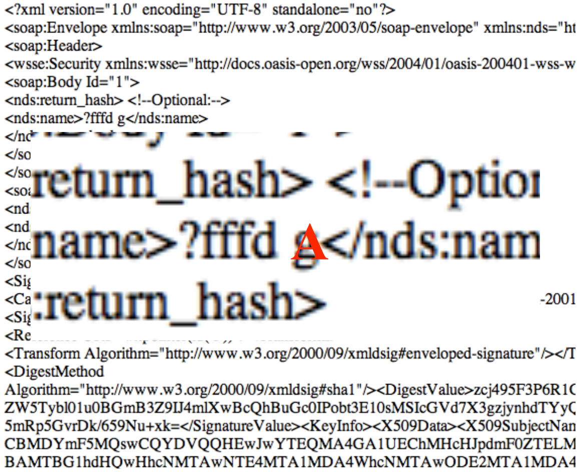


```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nd
</nc    return_hash> <!--Optior
</so
</so
<soa    name>?fffd g</nds:nam
<nd
<nd
</nc    :return_hash>
</so
<Sig
<Ca                                                                          -2001
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
<Reference URI="#xpointer(id('1'))"><Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C
ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC
5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan
CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM
BAMTBG1hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4
```

Signature Verification

VERIFIED ✔

BitFlip: controlled change of single character

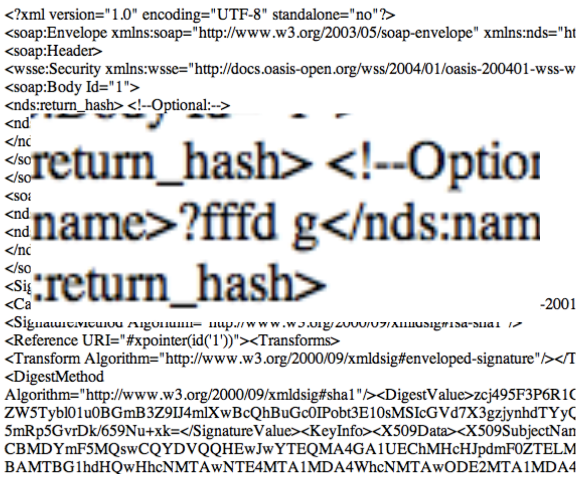


```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nds:name>?fffd g</nds:name>
</nc
</so    return_hash> <!--Optior
</so
<soa
<nd     name>?fffd A</nds:nam
<nd
</nc
</so    :return_hash>
<Sig
<Ca                                                                          -2001
<Sig
<Re
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C
ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC
5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan
CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM
BAMTBG1hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4
```

Signature Verification

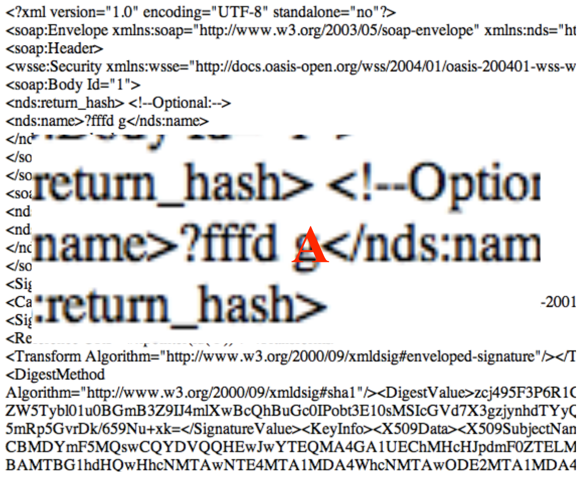
VERIFIED

BitFlip: Observing the Signature Verification Outcome on Application Induced Errors



```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nd
</nc
</so return_hash> <!--Optioı
</so
<so:
<nd name>?fffd g</nds:nam
<nd
</nc
</so
<Si :return_hash>
<Ca                                                                                 -2001
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
<Reference URI="#xpointer(id('1'))"><Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C
ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC
5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan
CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM
BAMTBG1hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4
```

BitFlip: controlled change of single character



```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nds:name>?fffd g</nds:name>
</nc
</so
</so return_hash> <!--Optioı
<so:
<nd
<nd name>?fffd A</nds:nam
</nc
</so
<Si
<Ca :return_hash>                                                                   -2001
<Si
<Re
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C
ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC
5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan
CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM
BAMTBG1hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4
```

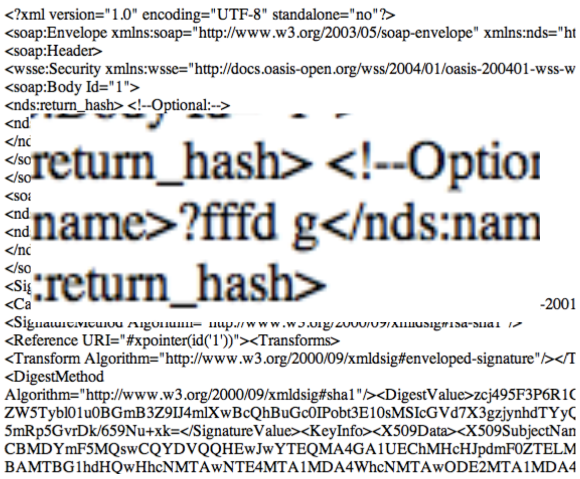
Signature Verification

VERIFIED ✓

Signature Verification

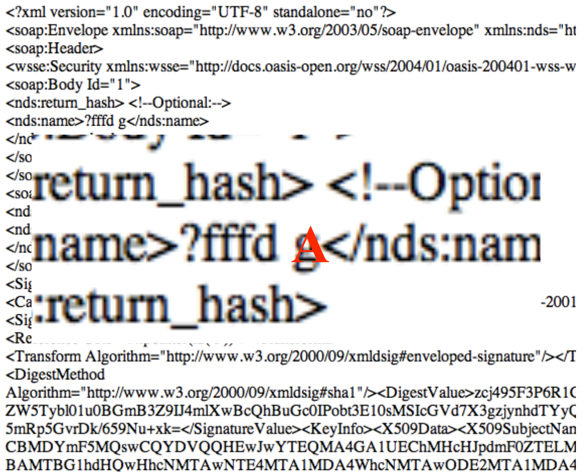
✗ VERIFIED

BitFlip: Observing the Signature Verification Outcome on Application Induced Errors



```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nd
</nc
</so
</so
<soa
<nd
<nd
</nc
</so
<Sig
<Ca                                                                        -2001
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
<Reference URI="#xpointer(id('1'))"><Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C
ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC
5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan
CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM
BAMTBG1hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4
```

```
return_hash> <!--Optior
name>?fffd g</nds:nam
:return_hash>
```



```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nds:name>?fffd g</nds:name>
</nc
</so
</so
<soa
<nd
<nd
</nc
</so
<Sig
<Ca                                                                        -2001
<Sig
<Re
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C
ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC
5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan
CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM
BAMTBG1hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4
```

```
return_hash> <!--Optior
name>?fffd gA</nds:nam
:return_hash>
```

BitFlip: controlled change of single character

Result: character not covered

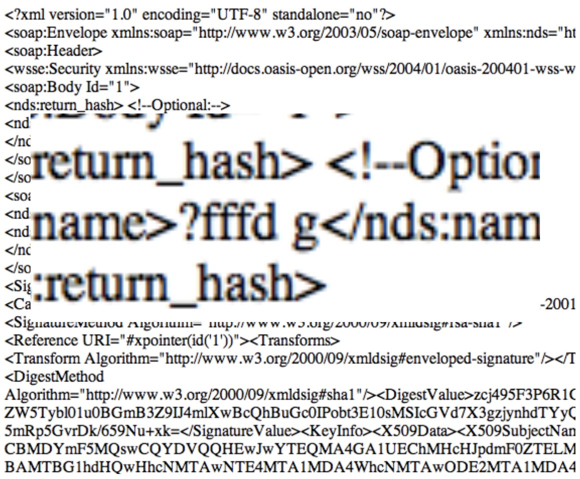
Signature Verification

VERIFIED ✔

Signature Verification

✗ **VERIFIED**

BitFlip: Observing the Signature Verification Outcome on Application Induced Errors

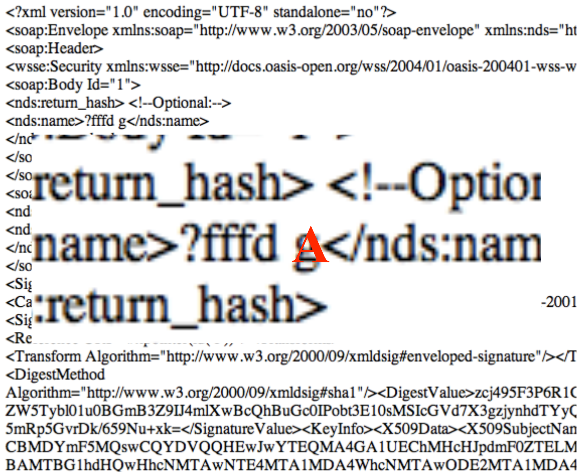


```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nd
</nc
</so return_hash> <!--Optior
</so
<soa
<nd  name>?fffd g</nds:nam
<nd
</nc
</so
<Sig :return_hash>
<Ca                                                         -2001
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
<Reference URI="#xpointer(id('1'))"><Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C
ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC
5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan
CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM
BAMTBG1hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4
```

Signature Verification

VERIFIED ✔

BitFlip: controlled change of single character

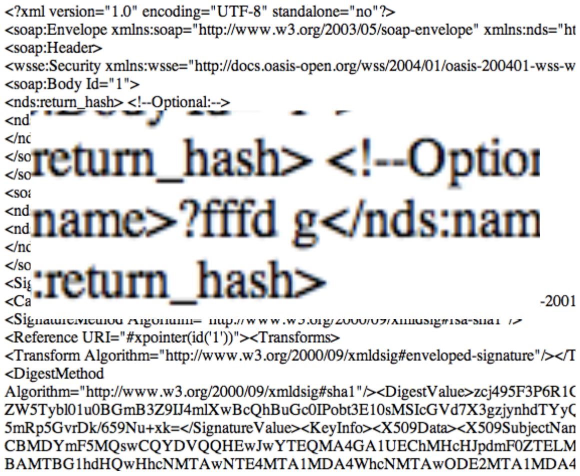


```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nds:name>?fffd g</nds:name>
</nc
</so
</so return_hash> <!--Optior
<soa
<nd
<nd  name>?fffd A</nds:nam
</nc
</so
<Sig
<Ca  :return_hash>                                          -2001
<Sig
<Re
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C
ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC
5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan
CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM
BAMTBG1hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4
```

Signature Verification

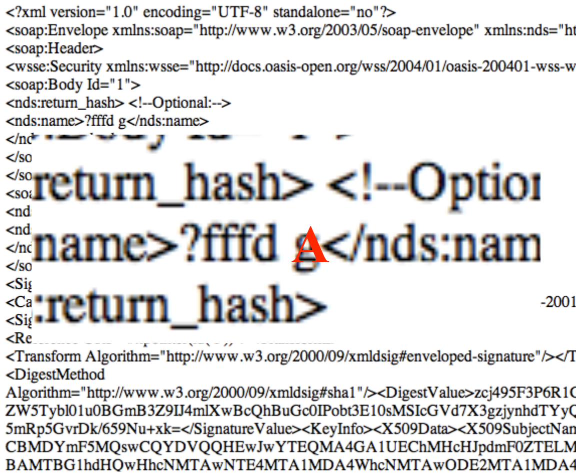
✔ FAILURE

BitFlip: Observing the Signature Verification Outcome on Application Induced Errors



```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nd
</nc
</so
</so
<soa
<nd
<nd
</nc
</so
<Sig
<Ca                                                                          -2001
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
<Reference URI="#xpointer(id('1'))"><Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C
ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC
5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan
CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM
BAMTBG1hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4
```

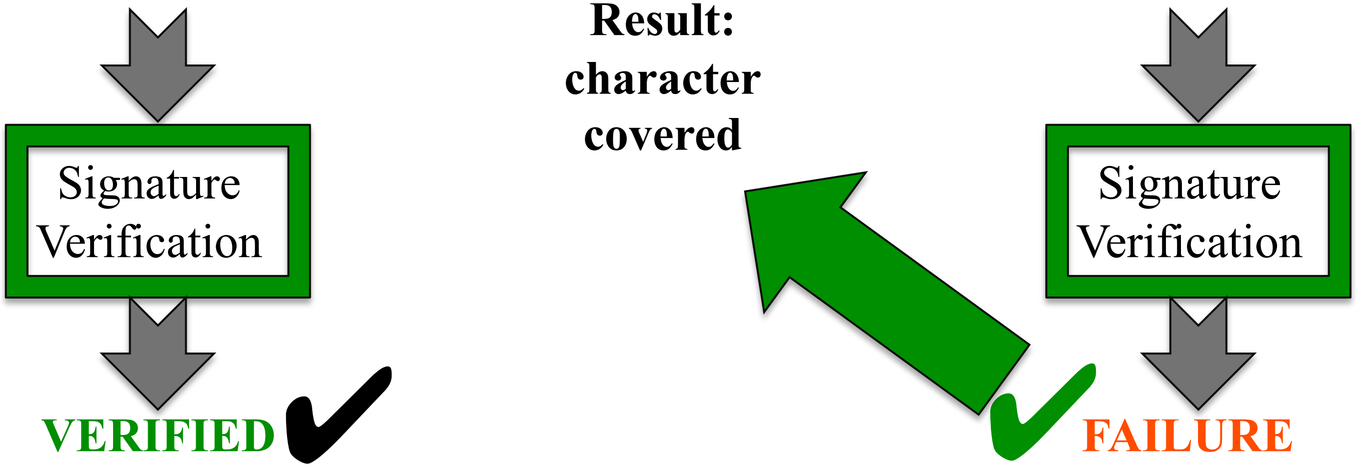
```
return_hash> <!--Optio
name>?fffd g</nds:nam
:return_hash>
```



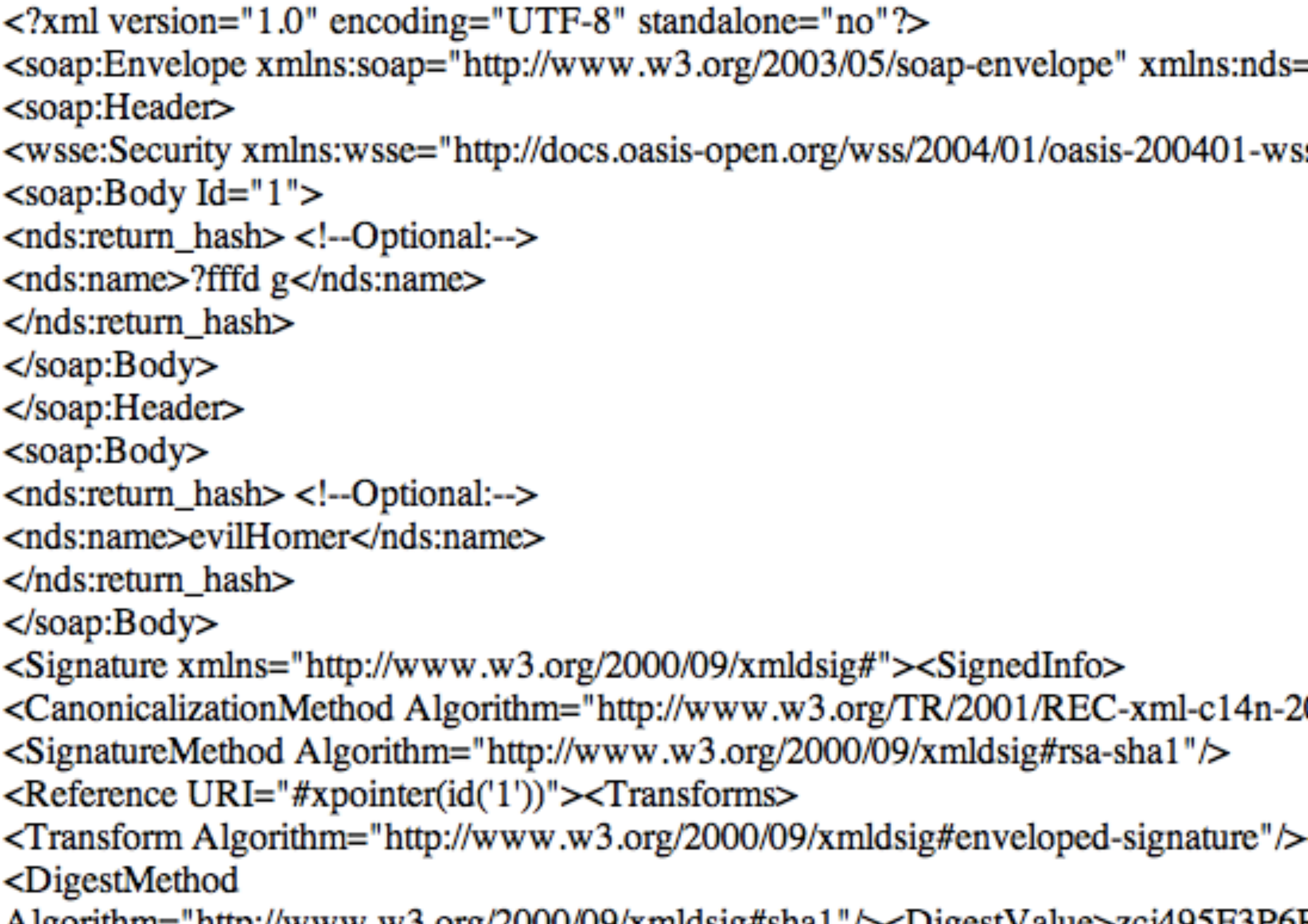
```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="ht
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-w
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nds:name>?fffd g</nds:name>
</nd
</so
</so
<soa
<nd
<nd
</nc
</so
<Sig
<Ca                                                                          -2001
<Sig
<Re
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/></T
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R1C
ZW5Tybl01u0BGmB3Z9IJ4mlXwBcQhBuGc0IPobt3E10sMSIcGVd7X3gzjynhdTYyC
5mRp5GvrDk/659Nu+xk=</SignatureValue><KeyInfo><X509Data><X509SubjectNan
CBMDYmF5MQswCQYDVQQHEwJwYTEQMA4GA1UEChMHcHJpdmF0ZTELM
BAMTBG1hdHQwHhcNMTAwNTE4MTA1MDA4WhcNMTAwODE2MTA1MDA4
```

```
return_hash> <!--Optio
name>?fffd g</nds:nam
:return_hash>
```

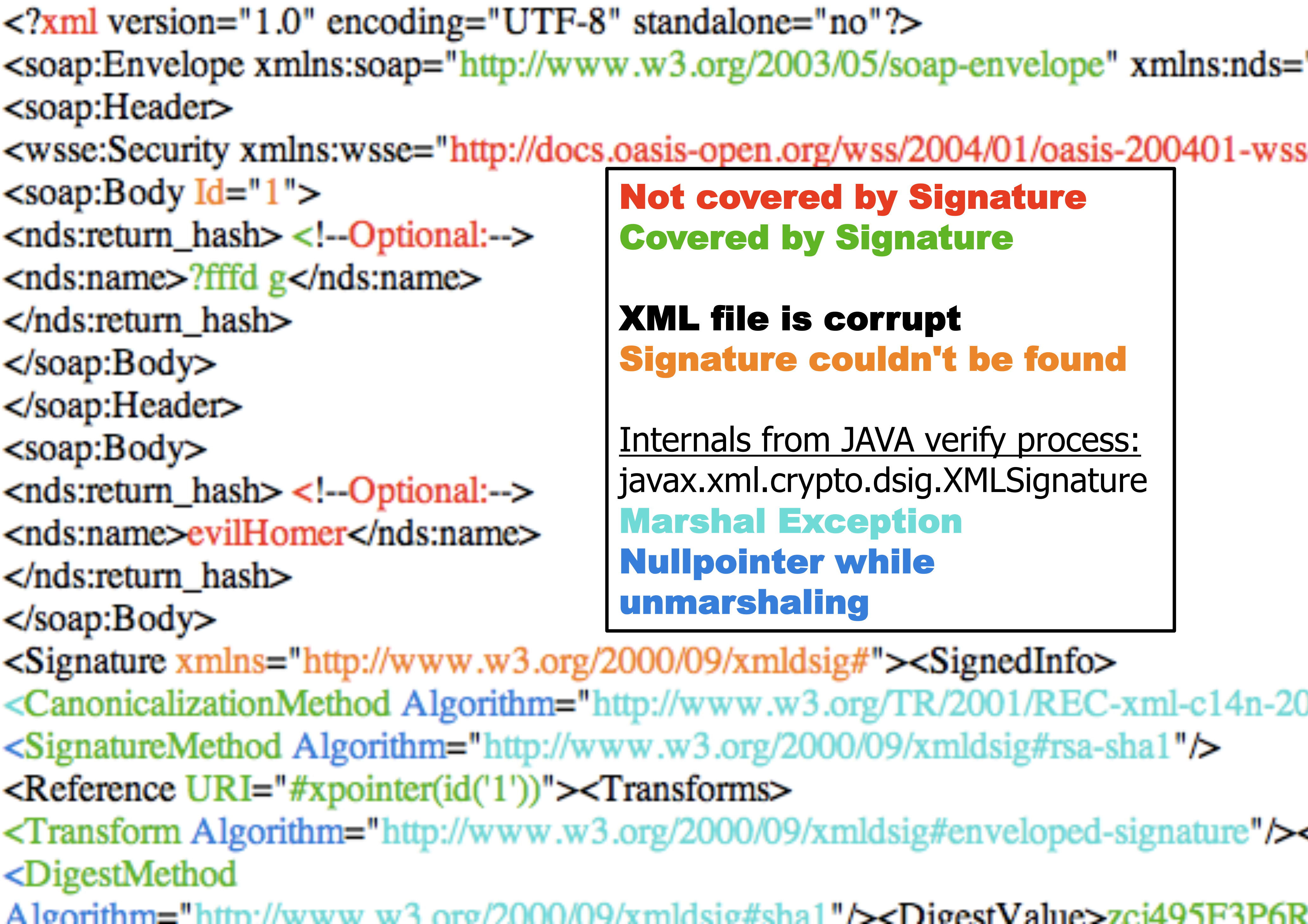
BitFlip: controlled change of single character



Result: character covered



```xml
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds=
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-ws
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nds:name>?fffd g</nds:name>
</nds:return_hash>
</soap:Body>
</soap:Header>
<soap:Body>
<nds:return_hash> <!--Optional:-->
<nds:name>evilHomer</nds:name>
</nds:return_hash>
</soap:Body>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-2
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<Reference URI="#xpointer(id('1'))"><Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zci495F3P6
```



```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nds:name>?fffd g</nds:name>
</nds:return_hash>
</soap:Body>
</soap:Header>
<soap:Body>
<nds:return_hash> <!--Optional:-->
<nds:name>evilHomer</nds:name>
</nds:return_hash>
</soap:Body>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<Reference URI="#xpointer(id('1'))"><Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/><
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zci495F3P6R
```

Not covered by Signature

Covered by Signature

XML file is corrupt

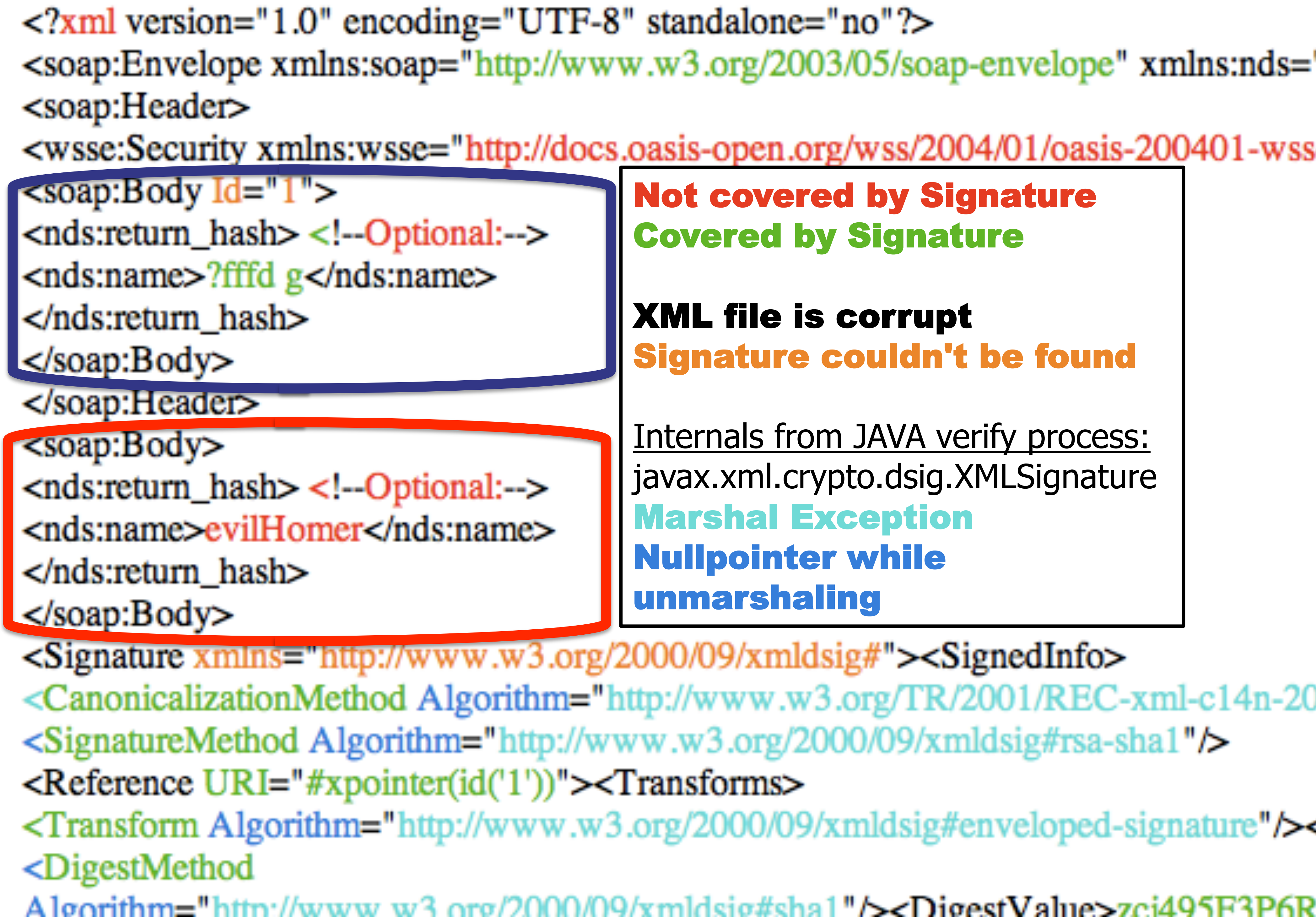
Signature couldn't be found

Internals from JAVA verify process:

javax.xml.crypto.dsig.XMLSignature

Marshal Exception

Nullpointer while unmarshaling



```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nds:name>?fffd g</nds:name>
</nds:return_hash>
</soap:Body>
</soap:Header>
<soap:Body>
<nds:return_hash> <!--Optional:-->
<nds:name>evilHomer</nds:name>
</nds:return_hash>
</soap:Body>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<Reference URI="#xpointer(id('1'))"><Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/><
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zci495F3P6R
```

Not covered by Signature

Covered by Signature

XML file is corrupt

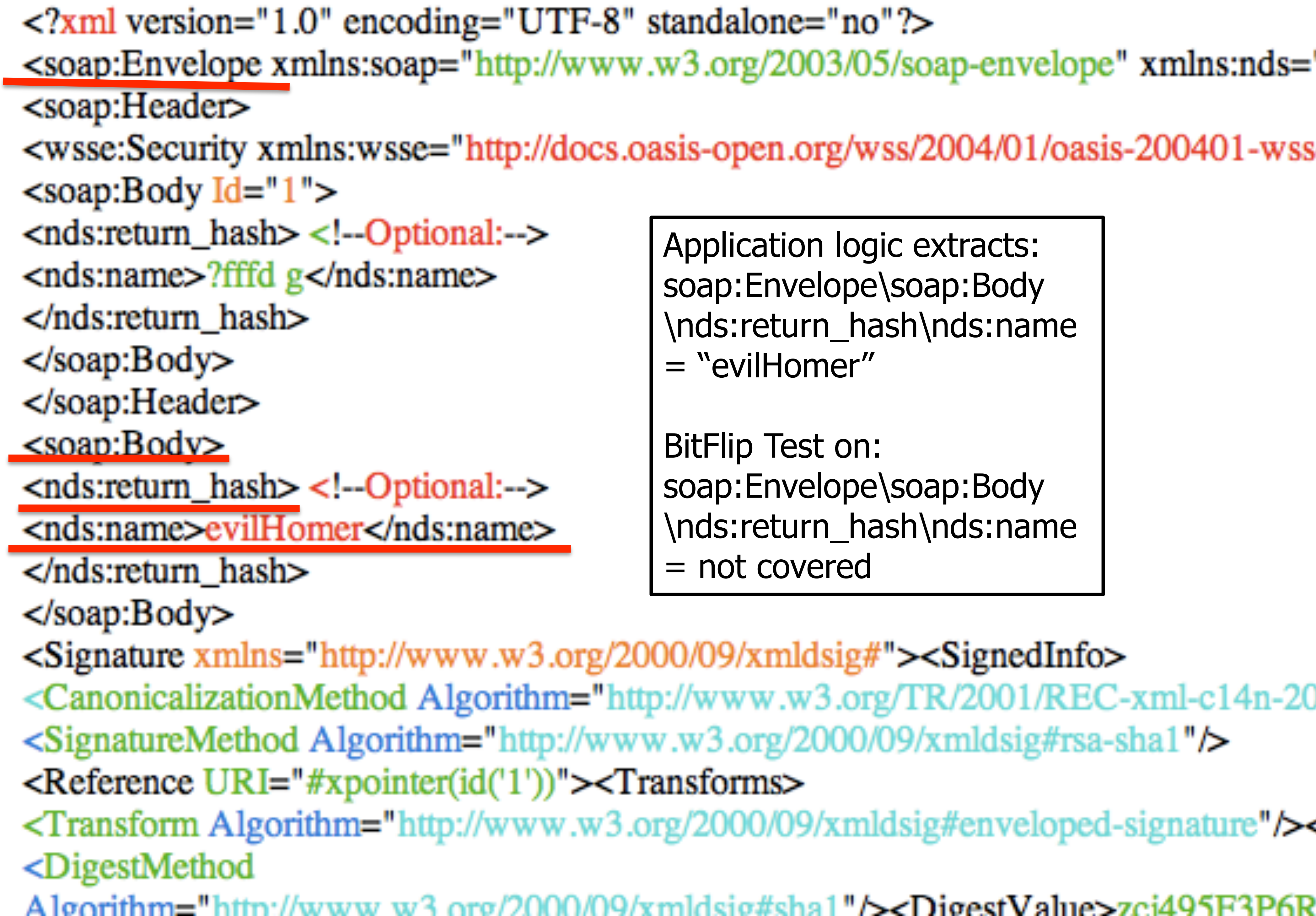
Signature couldn't be found

<u>Internals from JAVA verify process:</u>

javax.xml.crypto.dsig.XMLSignature

Marshal Exception

Nullpointer while unmarshaling



```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:nds="
<soap:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss
<soap:Body Id="1">
<nds:return_hash> <!--Optional:-->
<nds:name>?fffd g</nds:name>
</nds:return_hash>
</soap:Body>
</soap:Header>
<soap:Body>
<nds:return_hash> <!--Optional:-->
<nds:name>evilHomer</nds:name>
</nds:return_hash>
</soap:Body>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<Reference URI="#xpointer(id('1'))"><Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/><
<DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/><DigestValue>zcj495F3P6R
```

Application logic extracts:
soap:Envelope\soap:Body
\nds:return_hash\nds:name
= "evilHomer"

BitFlip Test on:
soap:Envelope\soap:Body
\nds:return_hash\nds:name
= not covered

What BitFlip does NOT and can NOT offer …

BitFlip does not do “positive verification”:

- no assurance that the parts that seem covered are secured against all kinds of attacks
- does not check for exploits in the signature verification process
- is not a “fuzzer”

What BitFlip does ...

- detects absence of integrity protection ("white spots")
- works independently of signature verification process ("black-box")
- implemented on application level
  - application controlled
  - use same "parser logic" to select flipping data
- absence can be detected by a single "flip"
  - overhead of one additional signature verification

BitFlip: Conclusion

- Allows Applications to test if Signature Verification Process covers the data the application logic extracted
- Independent of Verification Process (black-box)
  - Full Verification not necessary if no black-box
- Tool to evaluate the Verification Process
  - detect errors during application design
  - testing the layers below before application roll-out
  - re-run tests after changes to the policy or the verification process