

# VOEvent authentication via XML digital signature

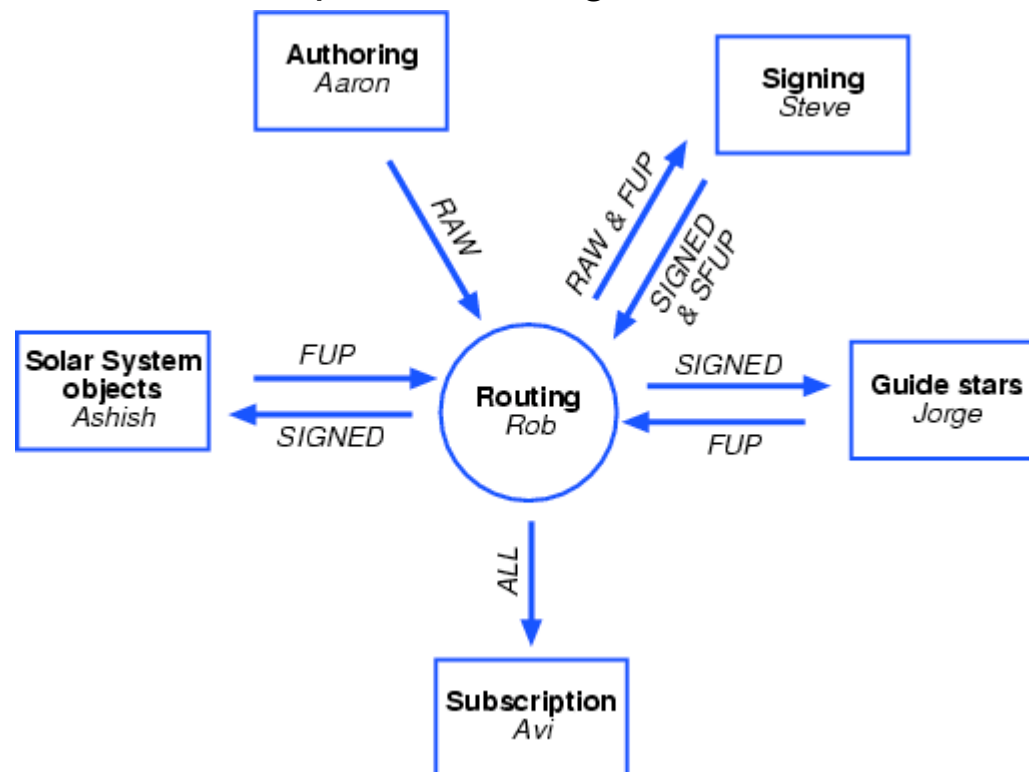


Steve Allen  
UCO/Lick Observatory

## Summer School Student Project Aspen, 2005 September

Team (in alphabetic order): Steve Allen, Avi Fhima, Jorge Garcia, Ashish Mahabal, Aaron Price, Rob Seaman

Aim: To demonstrate the generation, routing, signing, consumption and compilation of VOEvent packets using VO standards.



# What sort of actions might follow a VOEvent?

## Generation of RTML



## Words from previous sessions

Allan: relationships, trust

White: security will be needed

Williams: subscriber decision based on author

Borne: engage public, but no VOEvents from kids

Bloom: trust broker

# What's missing from VOEvent?

From RFC 4047 (FITS MIME)

## Security considerations:

FITS provides a means of transporting arrays and tables of data and keyword/value pairs of metadata. The standard FITS keywords are either mandatory or reserved. Mandatory keywords provide information necessary for correct interpretation of the data; reserved keywords merely provide standard bits of metadata. As such, the current standard FITS keywords do not pose security risks.

A FITS file author may insert additional keywords with semantics that are not described by the standard. Parties exchanging FITS files may employ locally defined conventions that use various keywords and their values to induce actions on the part of the recipient. There are existing local conventions where such keywords are used to request the reading of other files and/or URIs. There are other local conventions where such keywords are used to modify the state of a telescope and/or instrument. The security implications of local conventions such as these SHOULD be analyzed by the parties employing them.

**Required by IETF/IESG/IANA in every specification**

# VO has many doc types

## Why is VOEvent different?

- \_ Other VO protocols are client/server
- \_ Single Sign On can identify both ends
- \_ VOEvent is broadcast or subscribe
- \_ VOEvent might originate anywhere
- \_ VOEvent can imply instant response
- \_ RTML resembles VOEvent

# What could go wrong?

- \_ VOEvent spam
- \_ VOEvent forgery
- \_ RTML botnets
- \_ Hot-wiring the HTN Universe



# IETF/W3C already has solution

XML-Signature Syntax and Processing

W3C Recommendation 12 February 2002

<http://www.w3.org/TR/2002/REC-xmlsig-core-20020212/>

RFC 3275

Initiative started in 1999. It relies on alphabet soup of XML, Internet, and other standards. A partial list is DOM, SAX, SOAP, XLink, XML-C14N, XML-ns, XML-schema, XPath, XPointer, XSL, XSLT; DSS, MD5, PGP, SHA-1, X509v3; Unicode, UTF-16, UTF-8.

# Canonical XML

```
<?xml version="1.0"?>  
  
<?xml-stylesheet href="doc.xml"  
  type="text/xml" ?>  
  
<!DOCTYPE doc SYSTEM "doc.dtd">  
  
<doc>Hello, world!<!-- Comment 1 --></doc>  
  
<?pi-without-data ?>  
  
<!-- Comment 2 -->  
  
<!-- Comment 3 -->
```

```
<?xml-stylesheet href="doc.xml"  
  type="text/xml" ?>  
<doc>Hello, world!</doc>  
<?pi-without-data?>
```

```
<?xml-stylesheet href="doc.xml"  
  type="text/xml" ?>  
<doc>Hello, world!<!-- Comment 1 --></doc>  
<?pi-without-data?>  
<!-- Comment 2 -->  
<!-- Comment 3 -->
```

# Relevant info and tools

- \_ XML Signature WG
  - <http://www.w3.org/Signature/>
- \_ OpenSSL
  - To generate X509 certificate (with key)
- \_ XML Security Library (C)
  - <http://www.aleksey.com/xmlsec/index.html>
- \_ 2 other java, python, perl, + commercial

# diff from VOEvent 1.1

```
4a5
> xmlns:ds="http://www.w3.org/2000/09/xmlsig#"
8a10,12
> <xs:import namespace="http://www.w3.org/2000/09/xmlsig#"
>   schemaLocation="http://www.w3.org/TR/xmlsig-core/xmlsig-
core-schema.xsd"/>
>
22a27
>   <xs:element name="Signature" type="ds:SignatureType"
minOccurs="0" />
```

Declare the namespace. Import it.

Here `<Signature>` is an *optional* element which may occur 0 or more times.

That's all!

# example Signature element

The raptor event with XPath excluding all Signature elements and no cert

```
<Signature xmlns="http://www.w3.org/2000/09/xmlsig#">
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmlsig#rsa-sha1" />
<Reference>
<Transforms>
<Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
<XPath xmlns:dsig="http://www.w3.org/2000/09/xmlsig#">not(ancestor-or-
self::dsig:Signature)</XPath>
</Transform>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmlsig#sha1" />
<DigestValue>L/QfutJ3GbWxWOxCC0KBE7sTBIw=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>MM+HALvmY70WASCPi4e899bVWBOu+IZx4dW4wrRnmdhg1Zj1wQrfdZ02jqzcnl0
0
GzHC4JEulhXVfRNCqG5m2dN1abdKHLQQigG2+f01Rax/T0bjc0mj01Sjetd6KVec
7Tc76orELAHzTzLqG7q9wNZHLO9gdGzyvmfB7q33+Pc=</SignatureValue>
<KeyInfo>
<KeyName>ca.key</KeyName>
</KeyInfo>
</Signature>
```

# example Signature subelements

The raptor event with XPath excluding only its own Signature, plus cert

```
<Transforms>  
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>  
</Transforms>
```

```
<KeyInfo>  
<X509Data>  
<X509Certificate>MIIDuDCCAyGgAwIBAgIJAN4LhPm6nVZUMA0GCSqGSIb3DQEEBBAUAMIGaMQswCQYD  
VQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcn5pYTETMBEGA1UEBxMKU2FudGEgQ3J1  
ejEdMBsGA1UEChMUVUNPL0xpY2sgT2JzZXJ2YXRvcnkxDDAKBgNVBAsTA1NQRzEU  
MBIGA1UEAxMLU3RldmUgQWxsZW4xHjAcBgkqhkiG9w0BCQEW D3NsYUB1Y29saWNr  
Lm9yZzAeFw0wNzA2MDUwNTUzNTVaFw0wODA2MDQwNTUzNTVaMIGaMQswCQYDVQQG  
EwJVUzETMBEGA1UECBMKQ2FsaWZvcn5pYTETMBEGA1UEBxMKU2FudGEgQ3J1ejEd  
MBsGA1UEChMUVUNPL0xpY2sgT2JzZXJ2YXRvcnkxDDAKBgNVBAsTA1NQRzEUMBIG  
A1UEAxMLU3RldmUgQWxsZW4xHjAcBgkqhkiG9w0BCQEW D3NsYUB1Y29saWNrLm9y  
ZzCBnzANBghkiG9w0BAQEFAAOBjQAwGyKCGYEA t6lz/RZX8ToksKFLBN1GH2t1  
getWvs9Xy1UIfRcCxpFxn2HZXeE4/jd7f+SE/Jw6DHXDFIx+G1LHsUgc7CoOD7BF  
nOWhx9djbPYC8Jfnj4VFHBDfWjKQOQDSGBUTzFHPkmiQUiCwGnDhYZPR6jKJET9  
BjtYWFqZPM7dDKFZpqcCAwEAAaOCAQIwgf8wHQYDVR0OBBYEFKhdFKK3ld170s64  
2yRa/y7IvUwuMIHPBgNVHSMEgccwgcSAFKhdFKK3ld170s642yRa/y7IvUwuoYGg  
pIGdMIGaMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcn5pYTETMBEGA1UE  
BxMKU2FudGEgQ3J1ejEdMBsGA1UEChMUVUNPL0xpY2sgT2JzZXJ2YXRvcnkxDDAK  
BgNVBAsTA1NQRzEUMBIGA1UEAxMLU3RldmUgQWxsZW4xHjAcBgkqhkiG9w0BCQEW  
D3NsYUB1Y29saWNrLm9yZ4IJAN4LhPm6nVZUMAwGA1UdEwQFMAMBAf8wDQYJKoZI  
hvcNAQEEBQADgYEAiFAG8/YDME dD8uriVPyzS7E5ulrh268Oy37haZnbyFwV0vd6  
iJ0C/FM93Nr5fg16BJF135CyAH0ONQkG9GOvu6utbr1jGCe+GexSgRIwZCcKFoAh  
JkvhoL3Zg+zX26ObntJL+VQYFhUeHdq1claYocnPc4JXsFOQrrCUCda9oiw=</X509Certificate>  
</X509Data>  
</KeyInfo>
```

# What will be typical use patterns?

- \_ Signature is not required for any event.
- \_ For speed, initial VOEvent unsigned, identical followup comes with Signature?
- \_ Signatures could be added at any node.
- \_ Should Signatures sign previous ones?
- \_ Signatures need not always be verified.
- \_ Allows third party timestamping, proof.
- \_ VOEvent pipes could be open to amateurs (AAVSO), public, kids.

# VO's business is manufacturing epiphanies