

# Enveloped JSON Signatures

*Although XML Signatures are extremely flexible they come at a price: limited interoperability and mobile platform support. The case for XML has also been considerably weakened by REST which more or less has replaced SOAP for web-based systems used by for example Google and Facebook. In REST-based systems the returned data is usually in JSON format.*

## Converting to JSON

Due that I felt a need to convert the currently XML-based KeyGen2 system to JSON. However, there is currently no counterpart to XML DSig's enveloped signatures which made me develop such a system. It turned out that less than 3,000 lines of Java code were required to *Encode/Decode* and *Sign/Verify* JSON data:

<https://code.google.com/p/openkeystore/source/browse/#svn%2Flibrary%2Ftrunk%2Fsrc%2Forg%2Fwebpki%2Fjson>

I can now safely retire my 200,000+ lines Android port of Xerces ☺

Things that make JSON signatures simpler than XML DSig include:

- No attributes that must be sorted
- No namespaces
- No defaults
- No SOAP envelopes
- No WS-Security framework

Obviously there are complex systems that live or die by the use of XML DSig and XML Schema but KeyGen2 is not one of them...

The JSON parser mentioned also does a pretty good job for supporting conformance checking with intended messages though registered message types as well through strict property order and reference checks.

## Sample signature

```
{
  "TestSignatures":
  {
    "@jmsns": "http://example.com/signature",
    "Now": "2013-08-29T08:04:07+02:00",
    "HRT":
    {
      "RT1": "67",
      "YT":
      {
        "HTL": "656756#",
        "INTEGER": -689,
        "Fantastic": false
      },
      "er": "33"
    },
    "ARR": [],
    "BARR":
    [{
      "HTL": "656756#",
      "INTEGER": -689,
      "Fantastic": true
    },
    {
      "HTL": "656756#",
```

```

    "INTEGER": -689,
    "Fantastic": false
  }],
  "ID": "AqzjEouXabcUH5y5SwUw",
  "STRINGS": ["One", "Two", "Three"],
  "EscapeMe": "A\\n\\",
  "Intra": 78,
  "EnvelopedSignature":
  {
    "SignatureInfo":
    {
      "Algorithm": "http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256",
      "Reference":
      {
        "Name": "ID",
        "Value": "AqzjEouXabcUH5y5SwUw"
      },
      "KeyInfo":
      {
        "SignatureCertificate":
        {
          "Issuer": "CN=Demo Sub CA,DC=webpki,DC=org",
          "SerialNumber": 1377713637130,
          "Subject": "CN=example.com,O=Example Organization,C=US"
        },
        "X509CertificatePath":
        [

```

```

"MIIClzcCAx+gAwIBAgIGAUDGICcKMA0GCSqGSIb3DQEBCwUAMEMxEzARBgoJkiaJk/IsZAEZFgNvcmcxYjAUBgoJkiaJk/IsZAEZFgZ3ZWJwa2kxZDASBgNVBAMTC0RlbW8gU3ViIENBMB4XDTEyMDcxMDA5NTk1OVowQjE
LMAkGA1UEBhMCVVMxHjAeBgNVBAoTFEV4YVlwbGUgT3JnYW5pemF0aW9uMRQwEgYDVQDEwtleGFtcGxlLmNvbTBZMBMGB
yqGSM49AgEGCCqGSM49AwEHA0IABECkenu7FrOpy7J2FGe0lvtseQqJT2GsaExxK5UVKelzhFXjF+V8OFjv/FdM9fqdgw
kP/YUnx5epvvHh/+cQWjXTBbMAKGA1UdEwQCMAAwDgYDVROPAQH/BAQDAgP4MB0GA1UdDgQWBRR4YF2UOnLWDhOPLLuXY
Zum7xLMajAfBgNVHSMEGDAWgBRZXCf2vVvvaakHechUVh7jSlyIVTANBgkqhkiG9w0BAQsFAAOCAQEajBuZK2TcDhib12D
SW8rW3kyjFQ3iYtjNSvd7vJ5jyI+0OYQ/NlhN4vVjx7Z02vnrBxv1Nh9swgT5Jpw0724KawGC4P+/bUEvKVz89tPM19DaV
98yQ2YN4cBfhcW3FpAoI4dzBbCzfEplsh9Ek7VxuIgwPozl0AdqOmTjZ3hh54ApSq/PMwENDyCEzD6bvrCrqCjgWSYIQUI
vQ7Lf02HALEE9DcoV4mS1/8uiQ05hRdGmNYUHZVUua0HHX1h/nAS+IcS6/EDd89kEGrL3M92a5wqnIQvDLO2NBCXhHSxoP
VyBzv0lIga00ixD+q5P2OszRBYG3uk9W/uNIHdoyQn19w",

```

```

"MIIDZjCCAK6gAwIBAgICAMgwdQYJKoZIhvcNAQELBQAwRDETMDEBGCgmSjJomT8ixkARKWA29yZzEwMBQGCgmSjJomT8ixkA
RkWBndlyNBraTEVMBMGA1UEAxMMRGVtbyBSb290IENBMB4XDTEyMDcxMDA5NTk1OVowQzETMBE
GCgmSjJomT8ixkARKWA29yZzEwMBQGCgmSjJomT8ixkARKWBndlyNBraTEUMBGA1UEAxMLRGVtbyBTDWlGQ0EwggEiMA0GC
SqGSIB3DQEBAQUAA4IBDwAwggEKAoIBAQCQI1w6lq0AsHbWMes8i/UGBeVQnlbzL2N8VyLjkbT3HXNHPUTjWWQElhoRzFA
2xPaH++V/ecgr2DkievrM+B5yIsdAL4oWwmgZ9KVMSfOrl5jy843p6AA55CH1P4j8vluU1SpexIMUegDcNPlBwSRc0PPX+
uqQ1STRG0kUgi4Bap7U5IRxTvp06adFXU4Bjr85ML7VZ3j+164t6mLnwF5RChJm107aVuz6TwxnWqeZytjF0ei742dgbX9
SHPVvytLtbFp4V/VFoEhaOXLziOudPvpVwVdlfgE0AtiGHEWrfA74BU5XhME6UXzjcl3y3Ic304YGymo2jvmOwBki5wb3A
gMBAAGjYzBhMA8GA1UdEwEB/wQFMAMBAf8wDgYDVROPAQH/BAQDAgEGMB0GA1UdDgQWBRRZXCf2vVvvaakHechUVh7jSly
IVTAFBgNVHSMEGDAWgBRAQnES9aDCSV/XOk1JczxnqxI4/DANBgkqhkiG9w0BAQsFAAOCAQEAMlPdBaZ/+AMdfFYI9SLQe
nx0/vludp0oN9BSDe+mTfYnp5nS13lcZRCkMAR3g/zzgkULu022xTJVsXfM1dsMYwEpGZp+GAvrlmR06IathHW4aeo0Qpa
ygOgfquQNYgS3Z8OJRSUDGnoY65g50dgv11+ASbZX/r0/fNANLzXt/cnf0VXPrWdqvhUUS0561TsbTYg4qzcyDRV5vpjoU
AxjFna06TJkeZR/OYMcTtPRJON3/bMvzp7MfoL20PRPxu8nnqxwLWNzoQCKExS2yWHq1YDNNL4C/PIuyC/2IUbbPuwNp8
ir3MVBbq4QwuXbw6xFvbPxsOmZyH10xvpsnmokg",

```

```

"MIIDZjCCAK6gAwIBAgIBATANBgkqhkiG9w0BAQsFADBEMRMwEQYKCZImiZPyLQGGBGRYDb3JnMRYwFAYKCZImiZPyLQGGBG
RYGd2VicGtpMRUwEwYDVQDEwxEZwlvIFJvb3QgQ0EwHhcNMDIwNzEwMTAwMDAwWhcNMzAwNzEwMDk1OTU5WjBEMRMwEQY
KCZImiZPyLQGGBGRYDb3JnMRYwFAYKCZImiZPyLQGGBGRYGd2VicGtpMRUwEwYDVQDEwxEZwlvIFJvb3QgQ0EwggEiMA0GC
SqGSIB3DQEBAQUAA4IBDwAwggEKAoIBAQCmR4R0lJJyBUzQ92XDSzFuxiMjwFqsRkXUksIXMypjg2QZF4PzyQ0pu32/LV
Kuoaqbt+bkRKFdpUvMKhZGQ3rMathTukhXpFJN5Bk2LTcGXoE0B9wPkn4C3cxbUMetT94m8PKIjRoKm77Rvdd4vrG1GiCw
98WriMtNbX/psYzr/RikIcpEUpm4PPXzPPFuBzYIeDFG50aPEJu6arup5blw7Sqe6lq/f/XhKYWENH1LcQOFsMoQ8oUS/W
sYQ8aeT6/FxjMumjv4f9LanUhb73bBPA0xiqtEfniUk1ZogXgqT0157tqbmng2+GCSz+dGzv3VbSyQpdqh5s8YEGEK873vA
gMBAAGjYzBhMA8GA1UdEwEB/wQFMAMBAf8wDgYDVROPAQH/BAQDAgEGMB0GA1UdDgQWBRRZXCf2vVvvaakHechUVh7jSly
IVTAFBgNVHSMEGDAWgBRAQnES9aDCSV/XOk1JczxnqxI4/DANBgkqhkiG9w0BAQsFAAOCAQEAHyXu0Z74ZYbWdy/fUtI9u
Iid/7F5AjbdDtZJcZgbSvyF3ZYVF62pRjSyxtIcCKbbr/oRPF5voYzLI2PUL7HGBB1WzKDnfp5sXWwEC5kYmo7NrYxTzbg
22mS7nUpiRo07qr1FTM1aCaJhulRqioUKX4omlilZqTktQ61BmDODN+5RyBoA28EV+stt3+NV1JzOxIFqEqJfMWlq4Bzg5
RM/S4xy/jCj/hMSn2Etm5YoNVwju2L86JZ8433SoemQWjl7qMHEJ1tMEG9hR5DiE9j6STtbza+WbJHGqSdY/zlIsYbNgo
ZgYtJbRtZ4aObZb4Fxf1MTvObXiOInYgeKdK+Dw"

```

]

}



Author

[anders.rundgren.net@gmail.com](mailto:anders.rundgren.net@gmail.com)

2013-08-29