Pelmorex NAADS –
Alert Message Security using digital signatures

Issued March 17, 2010

2655 Bristol Circle
Oakville, Ontario L6H 7W1
T 905 829.1159
F 905 829.5800

Table of Contents

Table of Figures

Introduction

This document outlines the additional security mechanisms to the NAADS system to allow verification of the source of Alert Messages prior to on-air broadcasting by Last Mile Distributors (LMD).

Feedback and suggestions for improvement are encouraged from interested parties and should be sent to:

Attn: Paul Temple
Pelmorex Communications Inc.
2655 Bristol Circle
Oakville, ON L6H 7W1
Email: publicalerting@pelmorex.com
Phone: 905-829-1159 ext. 1271
Fax: 905-829-5800

The additional mechanisms are based on CAP, OASIS and XML standards and not tied to any vendor specific or custom solutions.

Additional Message Security

The additional message security will provide the following:

1. For any Alert issuer to stamp a specific Alert Message as a valid Message issued by their organization.
2. For any LMD to confirm (before processing any Message) that this is a valid Alert Message from NAADS system and also a valid Message from the issuing organization.

The additional security being added to NAADS consists of adding up to two digital signatures when an Alert Message is issued. The first signature will be from the Alert issuer and the second signature from the NAADS system. When an Alert is received, the Last Mile Distributor has the option of checking either or both of the signatures to validate that the Alert did originate from NAADS system (i.e. not tampered in internet transmission after issuing) and also validate that the original Alert Message from the issuer is genuine and intact (no change has been made to the content that was provided by the issuer in any form

Digital signatures are included in the CAP 1.2 specification and utilize the XML-Sig [1]standard. Digital signatures are used world-wide to secure access to documents and web transmissions. The XML-Sig standard identifies the various elements of the signature as below.

[1] Refer http://www.w3.org/TR/xmldsig-core/ for the XML-Sig standard

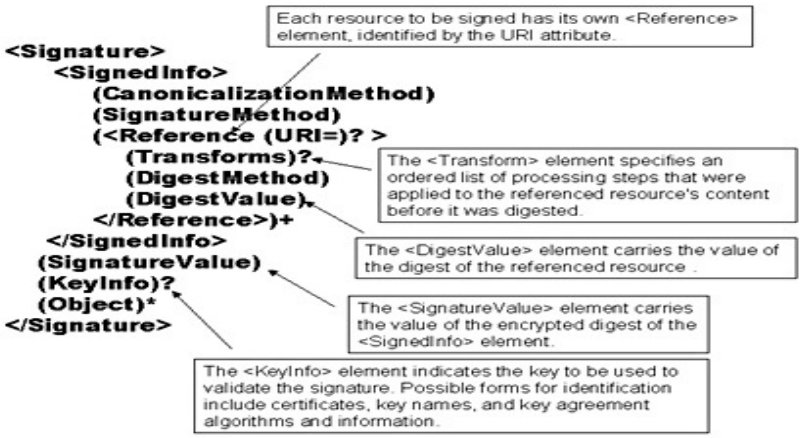

Figure 1 – Digital signature elements

For implementation of the digital signature, the OASIS Digital signing service standard[2] will be used both by NAADS and all participating Alert issuing organizations. OASIS-DSS defines a standard for a XML based service that can be maintained by any issuing organization/NAADS to apply digital signature to a submitted XML Message and to validate such a digitally signed Message. The LMD's that choose to validate the digital signatures will need to validate against the NAADS/Issuer DSS.

The OASIS-DSS standard was derived by the OASIS technical committee and included collaboration with major IT security vendors such as Entrust, IONA, NIST, webMethods, TIBCO. The Universal Postal Union has implemented DSS within its Electrical Post Mark system. Commercial OASIS-DSS solutions are provided by companies like ARX, Ascertia and Thales. An open-source implementation is found in the Sirius open source implementation package.

The XML-Sig standard also provides Signature ID property (that will be set by NAADS and issuers in their respective signatures) which can be used by XQuery/XSLT to include as well as exclude specific signatures. This allows for both independent verification of the signatures and for independent generation of two signatures. With this feature, the system provides the flexibility for Last Mile Distributors to ignore digital signatures, if they so choose.

End to End security provided by additional implementation

The end to end security for the whole NAADS system is provided by the above solution using the following industry standard security concepts:

1. **Securing the communication channel** using https.
2. **Authentication/authorization** provided through user name/password and infrastructure security.
3. **Authenticity/Non-repudiation** through digital signing of Alert Messages

[2] Refer http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss for the OASIS-DSS standard

The first two security measures from the list above are already implemented. The third feature will add additional security to the Alert dissemination as can be seen from Figure-3 in the next page.

- The digital signature adds another layer of security to the authentication/authorization. Even if a hacker fraudulently gains access to NAADS Alert interface through a compromised username/password and HTTPS secure connection – the additional step of signing the Alert will thwart their ability to issue any malicious Alert.

- Injection between NAADS issuing and NAADS dissemination – Before dissemination, NAADS validates a signed Message with the Issuer certification system for signature. This will identify tampered Messages and reject them.

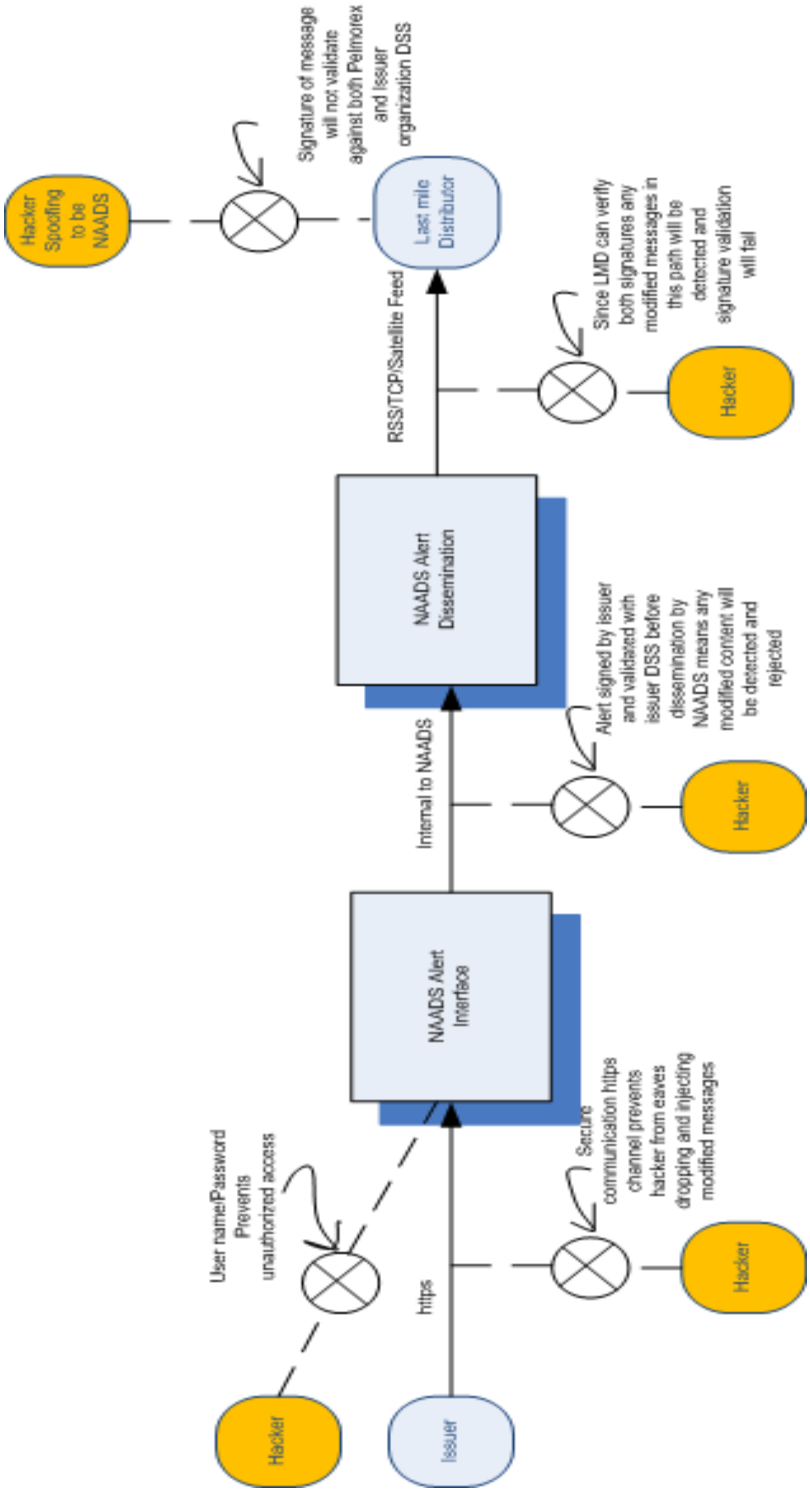

Figure 2 – New security solution – Additional security

- At the LMD end, the system protects against hackers spoofing to be NAADS and delivering Messages. This is no longer a risk as LMDs can check the second, i.e. NAADS signature to verify if it is from the NAADS system and reject it if otherwise. This can protect the LMD against any one injecting at the input of their own facility/system (even redistribution if they want to check the signature downstream in their operation).
- In addition, we encourage LMDs to also check the Issuer signature where it is included as a means to ensure the message itself is genuine and intact In this way the LMD can verify the issuer signature to double confirm if the original Alert Message has been modified/tampered at any point in the overall system.

Solution Details

The data flow for the overall solution is as follows (Refer to Figure 4 in next page)

1. Issuer creates Alert Message through the NAADS user interface (1 in drawing)
2. Issuer submits Alert Message for signing through the NAADS user interface to the DSS of their organization. The Message is signed and the issuer then submits it to NAADS central processing through the NAADS user interface (2 & 3)
3. NAADS central processing receives the Message. (4)
4. NAADS validates the signature by verifying against the issuer DSS (5 & 6). This guarantees no tampering in transmission. If the signature is not validated the Alert Message will be rejected and the issuer notified.
5. NAADS central processing adds its own signature using NAADS DSS (7 & 8)
6. Alert Message which has two signatures is delivered by various mechanisms to LMD (9&10). If issuer has no signing DSS, only NAADS signature will be appended to the Message.
7. LMD verifies the Message is sent by NAADS by validating NAADS digital signature against NAADS DSS. (11&12) This verifies that Message is not tampered in transmission from NAADS to LMD. If this is valid, then LMD can further validate that original Alert is not modified or tampered in any way from the original issuing source by validating the issuer's signature against the issuing organization DSS. (13 &14). For both these validations, the LMDs will need to form XML based http requests (following the OASIS-DSS standard) to the NAADS/Issuer DSS to get the signatures validated.
8. Once both validations are successful, the LMD can process the actual Alert Message. If the Message was signed only by NAADS, LMD will validate against NAADS DSS only.
9. LMD's that prefer to not process signatures can filter out both signatures using XQuery/XSLT.

The data flows for the validation part of the OASIS-DSS standard which mandates a service [3]that can validate signatures is shown in Figure 5.

[3] Refer http://www.oasis-open.org/committees/download.php/22721/ISSE-DSS-full-final-b.pdf for implementation of web service for digital signatures.

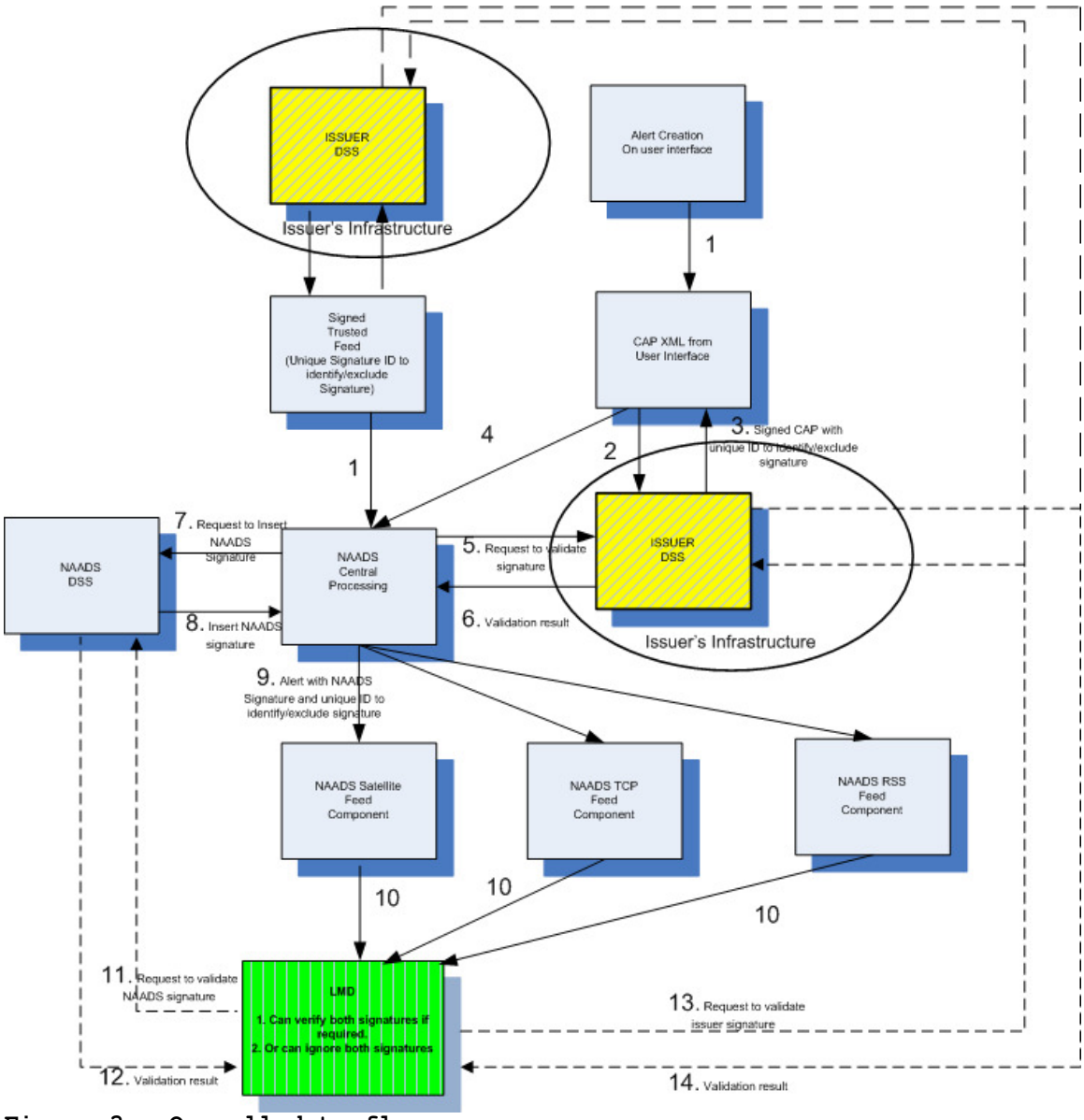

Figure 3 – Overall data flow

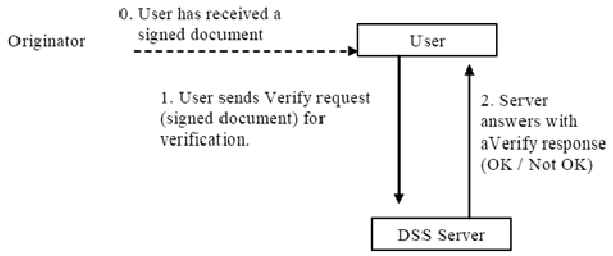

Figure 4 – Validating a signed message

Sample Messages

This section shows three sample CAP-CP Alert Messages.

- One unsigned Message as a reference
- Same Message with Issuer signature
- Same Message with Issuer + NAADS signature

Unsigned CAP Message

```
<?xml version="1.0" encoding="UTF-8"?>
<Alert xmlns="urn:oasis:names:tc:emergency:cap:1.2" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:oasis:names:tc:emergency:cap:1.2 http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.xsd">
	<identifier>3BEDC4EE50E642E395BE690F38CB5123</identifier>
	<sender>testSender@Pelmorex.com</sender>
	<sent>2009-12-03T16:09:00-00:00</sent>
	<status>Actual</status>
	<msgType>Alert</msgType>
	<source>PTINAADSFeedSocketSvc, NAADSFeed-dev01</source>
	<scope>Public</scope>
	<code>profile:CAP-CP:0.3</code>
	<info>
		<language>en-CA</language>
		<category>Met</category>
		<event>Thunderstorm</event>
		<responseType>Shelter</responseType>
		<urgency>Immediate</urgency>
		<severity>Extreme</severity>
		<certainty>Observed</certainty>
		<eventCode>
			<valueName>profile:CAP-CP:Event:0.3</valueName>
			<value>thunderstorm</value>
		</eventCode>
		<effective>2009-12-03T16:09:00-00:00</effective>
		<expires>2009-12-10T16:09:00-00:00</expires>
		<senderName>Pelmorex</senderName>
		<description>Thunderstorm Alert for Halton Region. This Message is a sample and is not a real Alert.</description>
		<area>
			<areaDesc>Halton Regional Municipality</areaDesc>
			<geocode>
				<valueName>profile:CAP-CP:Location:0.3</valueName>
				<value>3524</value>
			</geocode>

</area>
	</info>
</Alert>
```

Signed CAP Message with NAADS signature

```
<?xml version="1.0" encoding="UTF-8"?>
<Alert xmlns="urn:oasis:names:tc:emergency:cap:1.2" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:schemaLocation="urn:oasis:names:tc:emergency:cap:1.2
http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.xsd">
        <identifier>3BEDC4EE50E642E395BE690F38CB5123</identifier>
        <sender>testSender@Pelmorex.com</sender>
        <sent>2009-12-03T16:09:00-00:00</sent>
        <status>Actual</status>
        <msgType>Alert</msgType>
        <source>PTINAADSFeedSocketSvc, NAADSFeed-dev01</source>
        <scope>Public</scope>
        <code>profile:CAP-CP:0.3</code>
        <info>
                <language>en-CA</language>
                <category>Met</category>
                <event>Thunderstorm</event>
                <responseType>Shelter</responseType>
                <urgency>Immediate</urgency>
                <severity>Extreme</severity>
                <certainty>Observed</certainty>
                <eventCode>
                        <valueName>profile:CAP-CP:Event:0.3</valueName>
                        <value>thunderstorm</value>
                </eventCode>
                <effective>2009-12-03T16:09:00-00:00</effective>
                <expires>2009-12-10T16:09:00-00:00</expires>
                <senderName>Pelmorex</senderName>
                <description>Thunderstorm Alert for Halton Region. This Message is a sample and is not
a real Alert.</description>
                <area>
                        <areaDesc>Halton Regional Municipality</areaDesc>
                        <geocode>
                                <valueName>profile:CAP-CP:Location:0.3</valueName>
                                <value>3524</value>
                        </geocode>


                </area>
        </info>

<Signature xmlns=http://www.w3.org/2000/09/xmldsig# ID="NAADSSignature">
                <SignedInfo>
                        <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315#WithComments"/>
                        <SignatureMethod Algorithm="http://www.w3.org/2000/09/
xmldsig#dsa-sha1"/>
```

NAADS Signature LMD to validate against NAADS DSS

```
                        <Reference URI="">
                                <Transforms>
                                        <Transform Algorithm="http://www.w3.org/2000/09/
xmldsig#enveloped-signature"/>
                                </Transforms>
                                <DigestMethod Algorithm="http://www.w3.org/2000/09/
xmldsig#sha1"/>
                                <DigestValue>uooqbWYa5VCqcJCbuymBKqm17vY=</DigestValue>
                        </Reference>
                </SignedInfo>
                <SignatureValue>
KedJuTob5gtvYx9qM3k3gm7kbLBwVbEQRl26S2tmXjqNND7MRGtoew==
   </SignatureValue>
                <KeyInfo>
                        <KeyValue>
                                <DSAKeyValue>
                                        <P>
/KaCzo4Syrom78z3EQ5SbbB4sF7ey80etKII864WF64B81uRpH5t9jQTxe
Eu0ImbzRMqzVDZkVG9xD7nN1kuFw==
        </P>
                                        <Q>li7dzDacuo67Jg7mtqEm2TRuOMU=</Q>

<G>Z4Rxsnqc9E7pGknFFH2xqaryRPBaQ01khpMdLRQnG541Awtx/
XPaF5Bpsy4pNWMOHCBiNU0NogpsQW5QvnlMpA==
        </G>
                                        <Y>qV38IqrWJG0V/
mZQvRVi1OHw9Zj84nDC4jO8P0axi1gb6d+475yhMjSc/
BrIVC58W3ydbkK+Ri4OKbaRZlYeRA==
        </Y>

                </DSAKeyValue>
                        </KeyValue>
                </KeyInfo>
        </Signature>
</Alert>
```

Signed CAP Message with issuer and NAADS signature

```
<?xml version="1.0" encoding="UTF-8"?>
<Alert xmlns="urn:oasis:names:tc:emergency:cap:1.2" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xsi:schemaLocation="urn:oasis:names:tc:emergency:cap:1.2
http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.xsd">
        <identifier>3BEDC4EE50E642E395BE690F38CB5123</identifier>
        <sender>testSender@Pelmorex.com</sender>
        <sent>2009-12-03T16:09:00-00:00</sent>
        <status>Actual</status>
        <msgType>Alert</msgType>
        <source>PTINAADSFeedSocketSvc, NAADSFeed-dev01</source>
        <scope>Public</scope>
        <code>profile:CAP-CP:0.3</code>
        <info>
```

```
                <language>en-CA</language>
                <category>Met</category>
                <event>Thunderstorm</event>
                <responseType>Shelter</responseType>
                <urgency>Immediate</urgency>
                <severity>Extreme</severity>
                <certainty>Observed</certainty>
                <eventCode>
                        <valueName>profile:CAP-CP:Event:0.3</valueName>
                        <value>thunderstorm</value>
                </eventCode>
                <effective>2009-12-03T16:09:00-00:00</effective>
                <expires>2009-12-10T16:09:00-00:00</expires>
                <senderName>Pelmorex</senderName>
                <description>Thunderstorm Alert for Halton Region. This Message is a sample and is not
a real Alert.</description>
                <area>
                        <areaDesc>Halton Regional Municipality</areaDesc>
                        <geocode>
                                <valueName>profile:CAP-CP:Location:0.3</valueName>
                                <value>3524</value>
                        </geocode>
                </area>
        </info>
        <Signature xmlns=http://www.w3.org/2000/09/xmldsig# ID=”IssuerSignature”>
                <SignedInfo>
                        <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315#WithComments"/>
                        <SignatureMethod Algorithm="http://www.w3.org/2000/09/
xmldsig#dsa-sha1"/>
                        <Reference URI="">
                                <Transforms>
                                        <Transform Algorithm="http://www.w3.org/2000/09/
xmldsig#enveloped-signature"/>

                                </Transforms>
                                <DigestMethod Algorithm="http://www.w3.org/2000/09/
xmldsig#sha1"/>
                                <DigestValue>uooqbWYa5VCqcJCbuymBKqm17vY=</DigestValue>
                        </Reference>
                </SignedInfo>
                <SignatureValue>
KedJuTob5gtvYx9qM3k3gm7kbLBwVbEQRl26S2tmXjqNND7MRGtoew==
    </SignatureValue>
                <KeyInfo>
                        <KeyValue>
                                <DSAKeyValue>
                                        <P>
/KaCzo4Syrom78z3EQ5SbbB4sF7ey80etKII864WF64B81uRpH5t9jQTxe
Eu0ImbzRMqzVDZkVG9xD7nN1kuFw==
        </P>
```

Issuer Signature –LMD to validate against Issuer DSS

<Q>li7dzDacuo67Jg7mtqEm2TRuOMU=</Q>

<G>Z4Rxsnqc9E7pGknFFH2xqaryRPBaQ01khpMdLRQnG541Awtx/
XPaF5Bpsy4pNWMOHCBiNU0NogpsQW5QvnlMpA==
</G>
<Y>qV38IqrWJG0V/
mZQvRVi1OHw9Zj84nDC4jO8P0axi1gb6d+475yhMjSc/
BrIVC58W3ydbkK+Ri4OKbaRZlYeRA==
</Y>
</DSAKeyValue>
</KeyValue>
</KeyInfo>
</Signature>
<Signature xmlns=http://www.w3.org/2000/09/xmldsig# **ID=”NAADSSignature”>**
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315#WithComments"/>
<SignatureMethod Algorithm="http://www.w3.org/2000/09/
xmldsig#dsa-sha1"/>
<Reference URI="">
<Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/
xmldsig#enveloped-signature"/>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/
xmldsig#sha1"/>
<DigestValue>uooqbWYa5VCqcJCbuymBKqm17vY=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>
KedJuTob5gtvYx9qM3k3gm7kbLBwVbEQRl26S2tmXjqNND7MRGtoew==
</SignatureValue>
<KeyInfo>
<KeyValue>
<DSAKeyValue>
<P>
/KaCzo4Syrom78z3EQ5SbbB4sF7ey80etKII864WF64B81uRpH5t9jQTxe
Eu0ImbzRMqzVDZkVG9xD7nN1kuFw==
</P>
<Q>li7dzDacuo67Jg7mtqEm2TRuOMU=</Q>

<G>Z4Rxsnqc9E7pGknFFH2xqaryRPBaQ01khpMdLRQnG541Awtx/
XPaF5Bpsy4pNWMOHCBiNU0NogpsQW5QvnlMpA==
</G>
<Y>qV38IqrWJG0V/mZQvRVi1OHw9Zj84nDC4jO8P0axi1gb6d+475yhMjSc/BrIVC58W3ydbkK+Ri4OKba
RZlYeRA== </Y>
</DSAKeyValue>
</KeyValue>
</KeyInfo> </Signature></Alert>

NAADS Signature LMD to validate against NAADS DSS

**** **End of Document** ****