



XML Examples for DHZMC-TDF

DHZMC-TDF-Examples

Version 2021-NOV

December 1, 2022

Distribution Notice:

This document has been approved for Public Release and is available for use without restriction.

Table of Contents

Chapter 1 - Introduction	1
1.1 - Purpose	1
Chapter 2 - Example Files	2
2.1 - DHZMC-TDF-MultipleAssertions-TDO.xml	2

Chapter 1 - Introduction

1.1 - Purpose

This is an informative supplement for DHZMC-TDF. This document provides concrete examples of XML files implementing DHZMC-TDF elements and attributes.

Chapter 2 - Example Files

2.1 - DHZMC-TDF-MultipleAssertions-TDO.xml

```
<?xml-model href="../../../Schematron/DHZM/DHZM_XML.sch" type="application/xml" schematypens="http://purl.oclc.org/dsdl/schematron"?><?xml-model href="../../../Schematron/DHZMC-TDF/DHZMC-TDF_XML.sch" type="application/xml" schematypens="http://purl.oclc.org/dsdl/schematron"?><?xml-model href="../../../Schematron/BASE-TDF/BASE-TDF_XML.sch" type="application/xml" schematypens="http://purl.oclc.org/dsdl/schematron"?><?xml-model href="../../../Schematron/ANLYS/ANLYS_XML.sch" type="application/xml" schematypens="http://purl.oclc.org/dsdl/schematron"?><?xml-model href="../../../Schematron/IC-SF/IC-SF_XML.sch" type="application/xml" schematypens="http://purl.oclc.org/dsdl/schematron"?><tdf:TrustedDataObject xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

    xmlns:tdf="urn:us:gov:ic:tdf"
    xmlns:dhzm="urn:us:gov:ic:digitalhazmat"
    xmlns:sign="http://www.w3.org/2000/09/xmldsig#"
    xmlns:sfhashv="urn:us:gov:ic:sf:hashverification"
    xmlns:sf="urn:us:gov:ic:sf"
    xmlns:anlys="urn:us:gov:ic:anlysassert"
    xmlns="urn:us:gov:ic:tdf"
    xsi:schemaLocation="urn:us:gov:ic:tdf ../../Schema/DHZMC-TDF/DHZMC-TDF.xsd urn:us:gov:ic:digitalhazmat ../../Schema/DHZM/DHZM.xsd
urn:us:gov:ic:anlysassert ../../Schema/ANLYS/ANLYS.xsd urn:us:gov:ic:sf:hashverification ../../Schema/IC-SF/HashVerification.xsd"
    tdf:version="202111-DHZMC-TDF.202111"
    sf:DESVersion="202111">

    <tdf:Assertion tdf:scope="PAYL">
        <tdf:StructuredStatement>
            <dhzm:DigitalHazMatAssertion dhzm:DESVersion="202111">
                <dhzm:DigitalHazMat>This element describes an obfuscated payload which is either known or suspected to contain software or similar
data which could cause harm to information processing systems. It has been encapsulated to render it inert. Any attempt to decode
this payload outside a safe analysis environment may pose a danger to your system.</dhzm:DigitalHazMat>
            </dhzm:DigitalHazMatAssertion>
        </tdf:StructuredStatement>
    </tdf:Assertion>
    <tdf:Assertion tdf:scope="PAYL">
        <tdf:StructuredStatement>
            <dhzm:ProvenanceAssertion dhzm:DESVersion="202111">
                <dhzm:ContentCollectionTimestamp>2019-01-17T09:00:00Z</dhzm:ContentCollectionTimestamp>
                <dhzm:ContentSize>100</dhzm:ContentSize>
                <dhzm:ContentEncodedSize>100</dhzm:ContentEncodedSize>
                <dhzm:ContentEncodingMethod>XOR</dhzm:ContentEncodingMethod>
            </dhzm:ProvenanceAssertion>
        </tdf:StructuredStatement>
    </tdf:Assertion>
    <tdf:Assertion tdf:scope="PAYL">
        <tdf:StructuredStatement>
            <anlys:AnalysisAssertion analys:DESVersion="202111">
                <anlys:OriginContentFilename>SuperBadDigitalHazMat</anlys:OriginContentFilename>
                <anlys:KnownMalicious>true</anlys:KnownMalicious>
                <anlys:AnalysisMethodList>
                    <anlys:AnalysisMethod>Virus_Scan</anlys:AnalysisMethod>
                </anlys:AnalysisMethodList>
                <anlys:AnalysisMethodToolList>
                    <anlys:AnalysisMethodTool>
                        <anlys:AnalysisMethodToolName>ManualAnalysis</anlys:AnalysisMethodToolName>
                    </anlys:AnalysisMethodTool>
                    <anlys:AnalysisMethodTool>
                        <anlys:AnalysisMethodToolName>cpe:/a:nsa:ghidra:9.0</anlys:AnalysisMethodToolName>
                    </anlys:AnalysisMethodTool>
                </anlys:AnalysisMethodToolList>
            </anlys:AnalysisAssertion>
        </tdf:StructuredStatement>
    </tdf:Assertion>
</tdf:TrustedDataObject>
```

```

        </anlys:AnalysisMethodTool>
        <anlys:AnalysisMethodTool>
            <anlys:AnalysisMethodToolName>Other:cpe:/a:nsa:superghidra:10.0</anlys:AnalysisMethodToolName>
        </anlys:AnalysisMethodTool>
    </anlys:AnalysisMethodToolList>
    </anlys:AnalysisAssertion>
</tdf:StructuredStatement>
</tdf:Assertion>
<tdf:EncryptionInformation>
    <tdf:KeyAccess>
        <tdf:AttachedKey>
            <tdf:KeyValue>abcdefghijklmnop</tdf:KeyValue>
        </tdf:AttachedKey>
    </tdf:KeyAccess>
    <tdf:EncryptionMethod tdf:algorithm="SHA-256"/>
</tdf:EncryptionInformation>
<tdf:ReferenceValuePayload tdf:uri="bitcionstealer.gz.enc"
    tdf:mediaType="application/octet-stream"
    tdf:isEncrypted="true">
    <tdf:ReferenceValueBlock tdf:uri="bitcionstealer.gz.enc.p01" sfhashv:block="1"/>
    <tdf:ReferenceValueBlock tdf:uri="bitcionstealer.gz.enc.p02" sfhashv:block="2"/>
    <sfhashv:ContentEncodedHashVerification sfhashv:hashType="SHA-256">
        <sfhashv:TotalHash sfhashv:blockSize="134217728" sfhashv:totalBlocks="2">a8cd34e5e8472b6ac51c1ae1cab3fe06fad053beb8ebfd8977b010655bfdd3c3</sfhashv:TotalHash>
        <sfhashv:BlockHash sfhashv:block="1">e1232c608aa3e28350cebc98e47dfe784f966bd027ea376b7d4700fe6b07ea3d</sfhashv:BlockHash>
        <sfhashv:BlockHash sfhashv:block="2">f9fa8e46bd027ea376b7d47dc0758a48a4f96e68fe78e064700f700fe6b07ea3</sfhashv:BlockHash>
    </sfhashv:ContentEncodedHashVerification>
    <sfhashv:ContentDecodedHashVerification sfhashv:hashType="SHA-256">
        <sfhashv:TotalHash sfhashv:blockSize="134217728" sfhashv:totalBlocks="2">1e9e34e5e8472b6ac51c1ae1cab3fe06fad053beb8ebfd8977b010655bfdd3c3</sfhashv:TotalHash>
        <sfhashv:BlockHash sfhashv:block="1">4e5e608aa3e28350cebc98e47dfe784f966bd027ea376b7d4700fe6b07ea3d</sfhashv:BlockHash>
        <sfhashv:BlockHash sfhashv:block="2">2e3e8e46bd027ea376b7d47dc0758a48a4f96e68fe78e064700f700fe6b07ea3</sfhashv:BlockHash>
    </sfhashv:ContentDecodedHashVerification>
</tdf:ReferenceValuePayload>
</tdf:TrustedDataObject>
```