

# EGEE

## GRID SECURITY INCIDENT DATA MODEL AND FORMAT DEFINITION

---

Document identifier:	<b>draft-jra3-grid-incident-datamodel-02.doc</b>
Date:	<b>22/08/2005</b>
Activity:	<b>JRA3: Security</b>
Document status:	<b>DRAFT</b>
Document link:	<b><a href="https://edms.cern.ch/document/632017/">https://edms.cern.ch/document/632017/</a></b>

---

**Abstract:** The document proposes the Grid Security Incident data model and defines extensions to the general computer security incident description and exchange format IODEF.

### Document Log

Issue	Date	Comment	Author/Partner
0-1	2005-04-12	Grid Security Incident document spun off from the MJRA3.6	Yuri Demchenko

### Document Change Record

Issue	Item	Reason for Change

---

## CONTENT

<b>1. INTRODUCTION</b> .....	<b>4</b>
1.1. PURPOSE.....	4
1.2. APPLICATION AREA .....	4
1.3. REFERENCES .....	4
1.4. DOCUMENT EVOLUTION PROCEDURE.....	4
1.5. TERMINOLOGY .....	4
<b>2. USING IODEF FOR GRID SECURITY INCIDENT DESCRIPTION (UPDATE)</b> .....	<b>6</b>
2.1. IODEF AND INCIDENT HANDLING FRAMEWORK.....	6
2.2. INCIDENT REPORTING FORMAT REQUIREMENTS OVERVIEW.....	6
2.2.1. <i>The Incident Reporting Operational Model</i> .....	6
2.2.2. <i>General Format Requirements</i> .....	7
2.2.3. <i>Incident Report Content Requirements</i> .....	8
2.2.4. <i>Adopting FINE Incident Reporting Format for Grid</i> .....	8
<b>3. IODEF DATA MODEL STATUS UPDATE (VERSION 0.4)</b> .....	<b>9</b>
3.1. IODEF STRUCTURE AND TOP LEVEL ELEMENTS .....	9
3.2. IODEF EXTENSIONS FOR GRID AND WEB SERVICES .....	15
<b>4. SUMMARY</b> .....	<b>21</b>

## 1. INTRODUCTION

### 1.1. PURPOSE

The document presents updates and further development of Grid Security Incident data model and XML schema as extension to the IODEF incident description format that is used by CSIRTs for incident information exchange.

### 1.2. APPLICATION AREA

This document intends to provide information about current understanding about Grid Security Incident that can be used for building Incident Handling Systems and Incident information exchange.

### 1.3. REFERENCES

*[This subsection provides a complete list of all documents referenced elsewhere in the document.]*

[R1]	Grid Security Incident Handling and Response Guide <a href="http://computing.fnal.gov/docdb/osg_documents/0000/000019/002/OSG_incident_handling_v1.0.pdf">http://computing.fnal.gov/docdb/osg_documents/0000/000019/002/OSG_incident_handling_v1.0.pdf</a>
[R2]	MJRA3.4 - Grid Security Incident definition and exchange format. - <a href="https://edms.cern.ch/document/501422/1">https://edms.cern.ch/document/501422/1</a>
[R3]	User Registration and VO Membership Management Requirements document: <a href="https://edms.cern.ch/document/428034">https://edms.cern.ch/document/428034</a>
[R4]	Format for INcident information Exchange (FINE) <a href="http://www.ietf.org/internet-drafts/draft-ietf-inch-requirements-03.txt">http://www.ietf.org/internet-drafts/draft-ietf-inch-requirements-03.txt</a>
[R5]	The Incident Data Exchange Format Data Model and XML Implementation Document Type Definition - November 2004. - <a href="http://www.ietf.org/internet-drafts/draft-ietf-inch-iodef-03.txt">http://www.ietf.org/internet-drafts/draft-ietf-inch-iodef-03.txt</a>
[R6]	The Incident Object Description Exchange Format (IODEF) Implementation Guide - <a href="http://www.ietf.org/internet-drafts/draft-ietf-inch-implement-01.txt">http://www.ietf.org/internet-drafts/draft-ietf-inch-implement-01.txt</a>
[R7]	INCH-WG report at IETF63 - <a href="https://listserv.surfnet.nl/scripts/wa.exe?A2=ind05&amp;L=inch&amp;D=1&amp;O=D&amp;P=6245">https://listserv.surfnet.nl/scripts/wa.exe?A2=ind05&amp;L=inch&amp;D=1&amp;O=D&amp;P=6245</a>
[R8]	IDMEF (Intrusion Detection Message Exchange Format) I-D version 014 - <a href="http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-14.txt">http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-14.txt</a>
[R9]	IODEF Schema information page - <a href="http://www.uazone.org/demch/projects/iodef/">http://www.uazone.org/demch/projects/iodef/</a>

### 1.4. DOCUMENT EVOLUTION PROCEDURE

Sections 2 and 3 provide update on the Grid Security Incident definition and proposed description format based on IODEF. This stage is considered as a final in the development of the proposed data model and exchange format. Further development may occur in case of practical implementation of the proposed format in CSIRT or Grid operational security practice.

### 1.5. TERMINOLOGY

#### Glossary

EGEE	the Enabling Grids for e-Science project
JSPG	Joint Security Policy Group
OSG	Open Science Grid
GSIInc	Grid Security Incident
IODEF	Incident Object Definition and Description Format
CSIRT	Computer Security Incident Response Team
INCH-WG	IETF Working Group on extended INCident Handling
FINE	Format for INCident information Exchange
Malifactor	The person with malicious intents, e.g. intruder or attacker in the security incident.
Spoofing	A technique used to gain unauthorized access to computers, whereby the intruder sends requests indicating that the request is coming from a trusted host/site or user.

## **2. USING IODEF FOR GRID SECURITY INCIDENT DESCRIPTION (UPDATE)**

### **2.1. IODEF AND INCIDENT HANDLING FRAMEWORK**

IODEF (Incident Object Description and Exchange Format) [R5] is a standard used by CSIRTs world wide to exchange incidents information. IODEF is compatible with another format for Intrusion Detection Systems (IDS) the Intrusion Detection Message Exchange Format (IDMEF) [R8].

This section will explain how is IODEF is used for incident reporting and handling and provides suggestions for IODEF use for Grid Security Incidents description.

Importance of adopting one of standard format for Grid Security Incidents reporting is explained by the needs of Grid Operational Security services to cooperate with external CSIRTs in incident responses activities.

### **2.2. INCIDENT REPORTING FORMAT REQUIREMENTS OVERVIEW**

This section provides an overview of the recent Requirements for the Format for INcident information Exchange (FINE) [R4] produced by the IETF INCH-WG, which is considered relevant to the Grid Security Incident reporting and exchange format.

The requirement document defines the high-level functional requirements for a transport format to exchange incident reports, including general requirements to format, content, security, and related requirements to Incident Handling Systems. This abstract data representation is specified in another INCH-WG document IODEF Data model [R5].

The intent of FINE is to decrease the response time to incidents and facilitate by improving the ability of CSIRTs to process incident reports. The definition of a well-defined format will facilitate the exchange of incident reports across organizations, regions and countries by achieving these particular goals:

- to make the semantics of the report as clear and unambiguous;
- to ensure that the data has a well defined syntax;
- to ensure that the structure of the report allows easy categorization and statistical analysis;
- to ensure the verifiability of the integrity of the report, and the authenticity of the report source.

#### **2.2.1. The Incident Reporting Operational Model**

The FINE requirement draft describes the basic Incident response operational model (see picture 2.1 below).

Incident reports are generated, received and updated . For example, an organization may send an incident report to a Computer Security Incident Response Team (CSIRT) when an attack is detected. CSIRTs receive incident reports from customers or from other CSIRTs. The CSIRTs maintain these reports in an Incident Report Database in some format that may be specific to the CSIRT. The CSIRTs may process the reports to generate statistics, or investigate an incident further. As part of the investigation or as part of the reporting, the CSIRT may forward the incident report or parts of it to other CSIRTs. The CSIRTs may also receive results of investigation, or additional information related to currently active incidents from other CSIRTs. In the context of FINE, the incident reports will be handled by a CSIRT via an interface that is capable of converting a FINE formatted incident report into the internal format used by the CSIRT and vice versa.

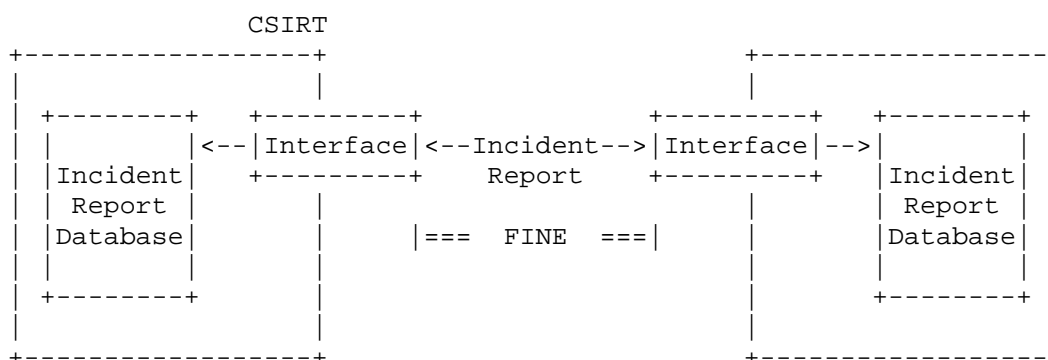


Fig. 2.1. Operational Model for FINE

From the operational point of view during the life-cycle of an incident report the following may apply:

- the report itself evolves. It may exist in one of the following states:
  - handling - the incident report is being handled
  - complete/closed - the incident report has been processed
  - and no further processing is planned
  - waiting - the incident report is waiting on some event;
- the report is exchanged between CSIRTs and may be investigated/processed by multiple CSIRTs, simultaneously;
- additions and/or changes to the report may be made by one or more CSIRTs. Therefore, a single CSIRT may not be in a position to vouch for the veracity of all parts of the incident report.

### 2.2.2. General Format Requirements

The following general Incident reporting format requirements are specified:

- FINE SHALL support full internationalization and localization and use of multiple languages.
 

A significant part of the incident report will be comprised of human readable text. Since some incidents will entail involvement of CSIRTs from different countries and geographic regions, FINE must have provisions for using local character sets and encodings.

In cases where local (non-standard) character sets and encodings are used, the elements that carry encoding sensitive information should be clearly indicated. It should be possible to preserve the content of these elements when transferring an incident report.
- FINE MUST be able to document the evolution of an incident.
 

An incident report may evolve with time, as further investigation is performed on the incident report. Earlier information may be modified and new information may be added. FINE must support the recording of these changes.
- FINE MUST support specifying a granular access restriction policy for the specific elements of the incident report.
 

Various parts of an incident report will have information of varying degrees of sensitivity and will need to be handled with the appropriate level of confidentiality. It must be possible to specify the degree of confidentiality for the individual components of the incident report. Applications can

then implement different levels of access restrictions for the different components of the incident Report.

### **2.2.3. Incident Report Content Requirements**

FINE specifies the following requirements to the Incident report content which are also applicable for the Grid Security Incident description:

1. FINE MUST support globally unique identifiers for each incident report.  
It should be possible to reference an incident report unambiguously using a globally unique identifier. It should be possible to derive the creator of the incident report from this identifier.
2. FINE MUST include the identity of the creator of the incident report.  
FINE should indicate the source of each component of the incident report if it is different from the creator (e.g., the team handling the incident).
3. FINE MUST be flexible enough to support various degrees of completeness, while still clearly defining the minimal information required for describing an incident.  
FINE SHOULD support the including or referencing information external to the incident report.
4. FINE SHOULD support the description of various aspects of the source and target.
5. FINE SHOULD contain a description of the methodology used in the attacker.  
Well-known classifications or enumeration schemes should be used to describe the attack or exploited vulnerabilities that caused the incident.  
FINE SHOULD support references to the appropriate advisories from coordination and analysis centers.
6. FINE SHOULD provide for describing the impact of the incident report.
7. FINE SHOULD support describing the actions taken during the course of handling an incident.

### **2.2.4. Adopting FINE Incident Reporting Format for Grid**

FINE requirements are enough general to provide a guidance for various application areas including Computer Grids and XML Web Services in general.

Based on overview and initial analysis above, it can be suggested that the FINE requirements can be adopted in general for Grid Security Incidents reporting.

However, this new area of use can provide even better integration between Incident reporting facilities and applications and their monitoring and logging system because of XML based nature of interactions in Web Services and Grids.



### 3. IODEF DATA MODEL STATUS UPDATE (VERSION 0.4)

IODEF is the product of the IETF INCH-WG which combines efforts of CSIRT community worldwide to define a common standard for security incidents description and exchange format.

Recent version of the IODEF Data model is version 0.4 which updates the last published draft on version 0.3 with new features that were discussed at the last INCH-WG meeting on March 9, 2005 at IETF-63.

The following improvements were proposed and design issues have been resolved [R7]:

- Version 0.4 signifies moving from XML DTD for IODEF Data model definition to XML Schema what intends to simplify extensions management and adding XML based security features.
- “iodef” namespace is introduced for the major IODEF datamodel.
- Design suggestions and recommendations for using XML Signature and XML Encryption were provided.
- Definition of name related elements in the Contact element has been updated
- Content of the System element that describes the system(s) involved in the incident is updated and extended with the User element and the OperationSystem element. Note: This is the place where the XMLWebService element is included.
- Semantics of the RecordData element that contains important collected data related to the incident is specified to allow use of rare log data, system files or other rare evidence information.

IODEF extension for Grid Security Incidents descriptions are proposed in a form of IODEF special profile for XML Web Services and Grids with the namespace “iodef-xws” discussed in details below. The work on IODEF-XWS profile definition is directly associated with the JRA3 operation security activity for EGEE.

Extending IODEF adoption as a common basic format for security incidents description is indicated by two another proposed IODEF profiles for Real-Time Internet Defence (RID) and for phishing [R7].

#### 3.1. IODEF STRUCTURE AND TOP LEVEL ELEMENTS

This section provides the update for the basic IODEF data model and provides information about the IODEF top-level elements. This is also an update of the related section of the MJRA3.4 document [R2].

The IODEF is designed to represent all necessary information about the computer security incident during its whole lifetime in a structured way using XML. The following element definitions are provided according to the recently updated IODEF data model specification version 0.4 [R5, R9].

The top level element IODEF-Document serves as a container for only one element: Incident. The Incident element contains all the incident-related information. It provides a standardized representation for commonly exchanged incident data and associates a unique identifier with the described activity.

The Incident element contains the following sub-elements and has the following structure as represented in the XML DTD format:

```
<!ELEMENT Incident (IncidentID, AlternativeID?, RelatedActivity?,  
Description*, Contact+, ReportTime, DetectTime?, StartTime?, EndTime?,  
EventData*, Method*, Expectation*, Assessment+, History?, AdditionalData*)>
```

**IncidentID** - an incident tracking number assigned to the incident by the party that generated the document.

**AlternativeID** - a list of incident tracking numbers used by other CSIRTs to refer to the same activity as described in the document.

**RelatedActivity** - a list of incident tracking numbers referencing related incidents.

**Description** - a free-form textual description of the incident activity.

**Contact** - contact information for the parties involved in the incident.

**DetectTime, StartTime, EndTime, ReportTime** - time information when the incident activity was correspondently first detected, started, ended, reported.

**EventData** - details on the data on the (security) events that lead to the incident.

**Method** - the techniques (e.g., tools, vulnerabilities) used by the attacker.

**Expectation** - expected action to be performed by the recipient (CSIRT) of the document.

**Assessment** - a characterization of the impact of the incident activity.

**History** - documents significant events or actions that occurred during the course of handling the incident.

**AdditionalData** - extension area for data that cannot be represented anywhere else.

Graphically the top level IODEF structure can be represented in a form of diagram Fig. 3.1.

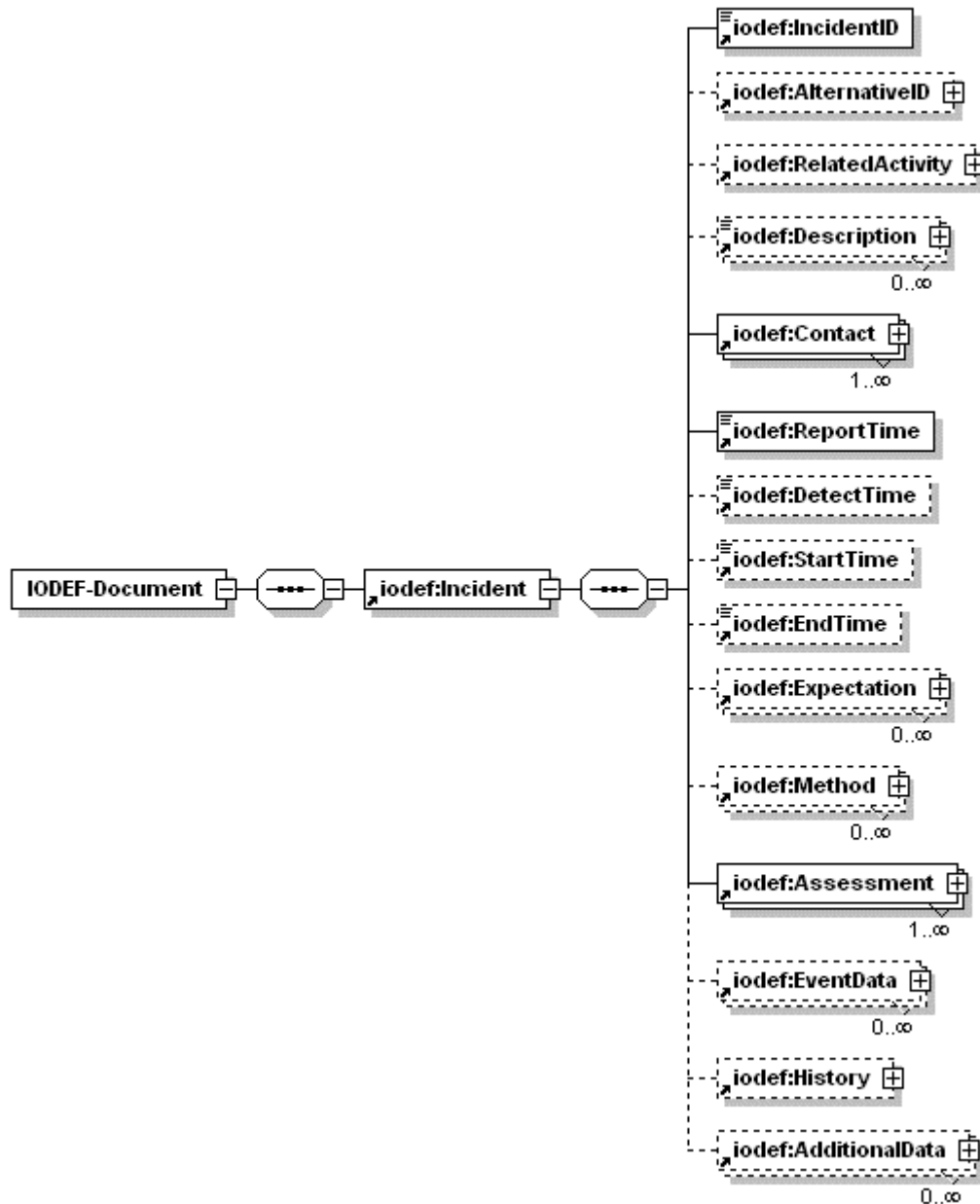


Fig. 3.1. The top level IODEF elements.

The Incident element may contain “zero” or “many” EventData elements where the actual incident data are contained. The EventData element has the following structure (see also Fig. 3.2):

```

<!ELEMENT EventData (Description*, Contact*, DetectTime?, StartTime?,
EndTime?, Flow*, System*, Method*, Assessment?, EventData*, Record?,
AdditionalData*)>
  
```

where most of the components are the same as in the higher level Incident element and two new elements are defined:

Flow – represents set/collection of similar events that may originate from the same of different Systems and applications.

System - the systems (nodes, networks) involved in the event as either sources, targets or intermediaries.

Record - support data (e.g., log files) that provides information about the events.

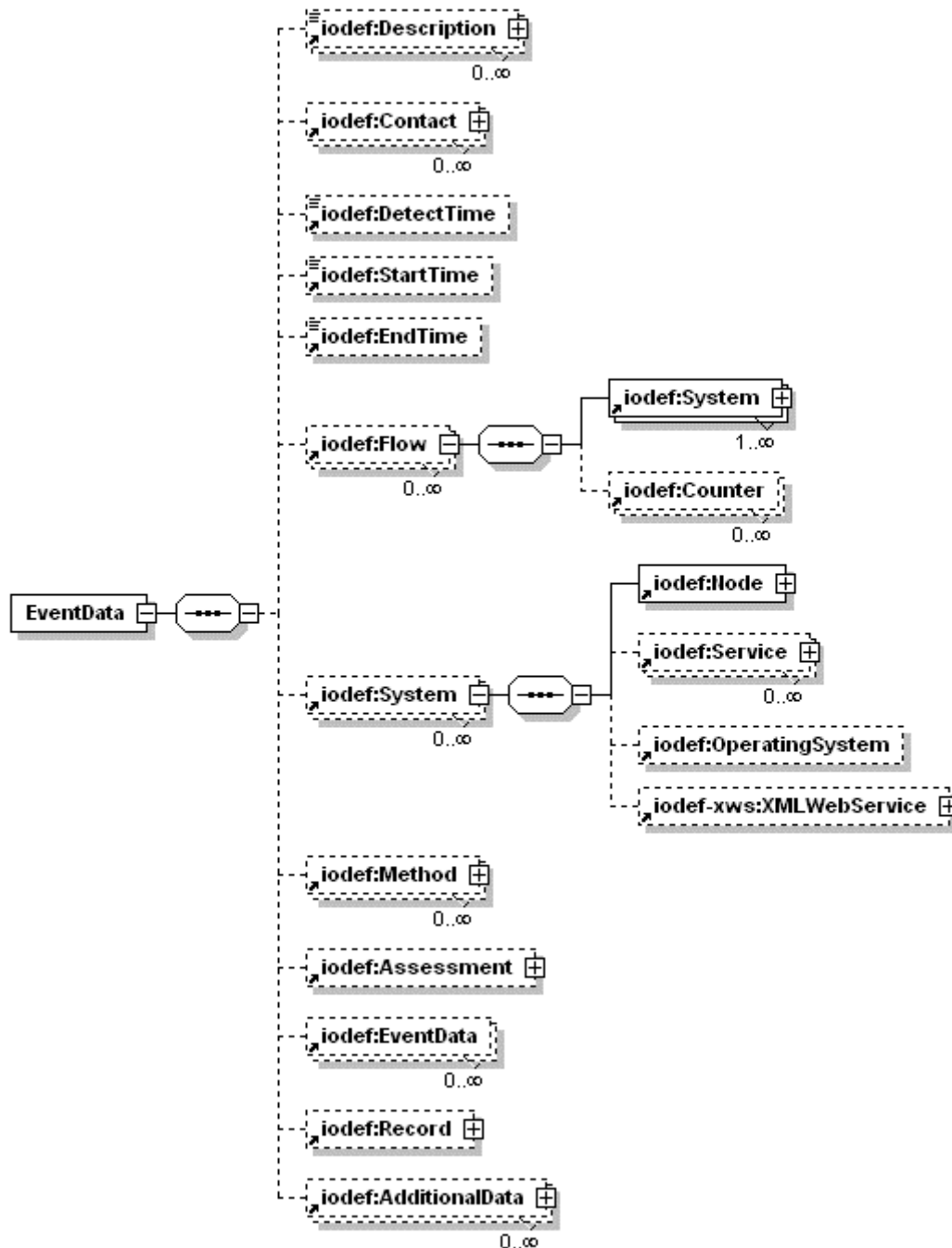


Fig. 3.2. The EventData element structure

The Record element may contain one or more RecordData elements that have the following structure (see also Fig. 3.3):

```

<!ELEMENT RecordData (DateTime?, Description*, Sensor?, Pattern?,
PatternLocation*, Counter?, RecordItem?)>
<!ATTLIST RecordData
  restriction NMTOKEN #IMPLIED
  reccourcetype CDATA #IMPLIED
>
  
```

**DateTime** - timestamp information for the RecordItem data.

**Description** - free-form textual description of the provided RecordItem data. At minimum, this description should convey the significance of the provided RecordItem data.

**Sensor** - information about the Sensor as a source of the data contained in the RecordData element. In particular case it can be Intrusion Detection System (IDS) or other intelligent event analyser. Other sources of the RecordData can be identified by the “reccourcetype” attribute.

**RecordItem** - log, audit, or forensic data.

**Pattern** – a pattern in the RecordItem data that identifies a specific incident signature.

**PatternLocation** – information that points on the location of pattern in the RecordItem data.

**Counter** – a number of pattern occurrence in the RecordItem data.

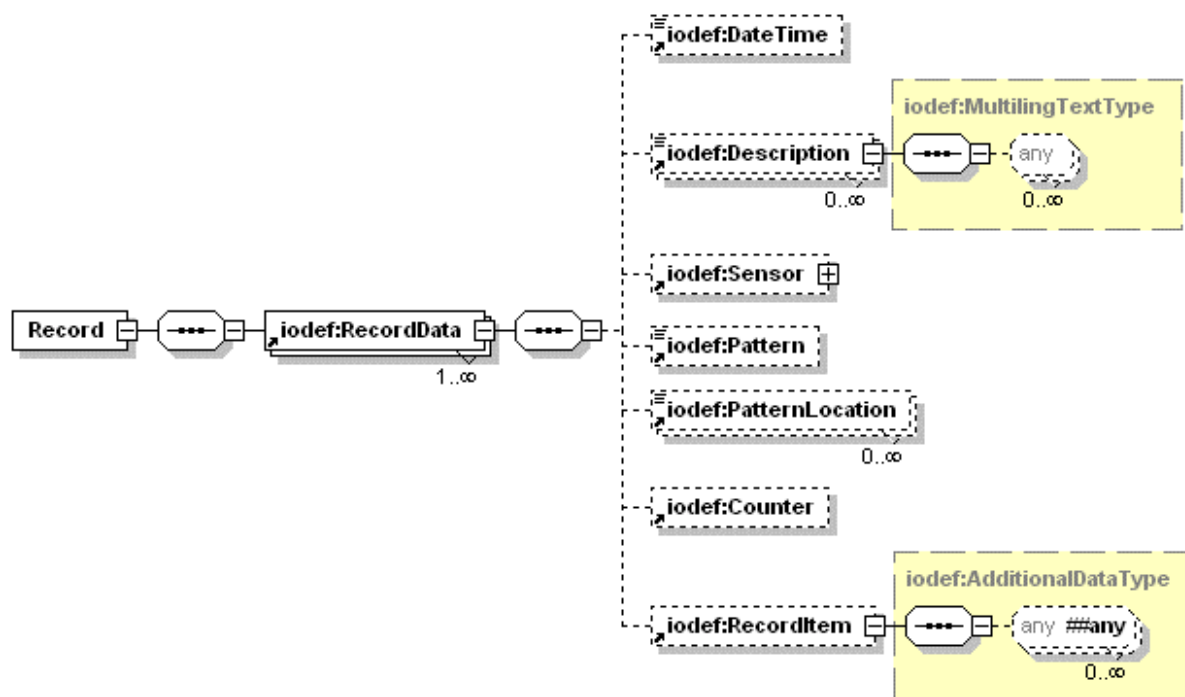


Fig. 3.3. The Record and RecordData elements structure

The System element contains the following sub-elements (see also Fig. 4.4.2):

```

<!ELEMENT System (Node, Service*, OperatingSystem*, XMLWebService*)>
  
```

**Node** - a host or network involved in the incident activity.

**Service** - the network service targeted on the host specified in Node.

**OperatingSystem** – information about the operating system installed on the Node or running the Service.

**XMLWebService** – description of the WML Web Service or Grid System in particular that was involved in the incident.

The elements XMLWebService is added as a child element to the System element to describe information specific for the Grid security incidents, they are described in detail in the next section.

### 3.2. IODEF EXTENSIONS FOR GRID AND WEB SERVICES

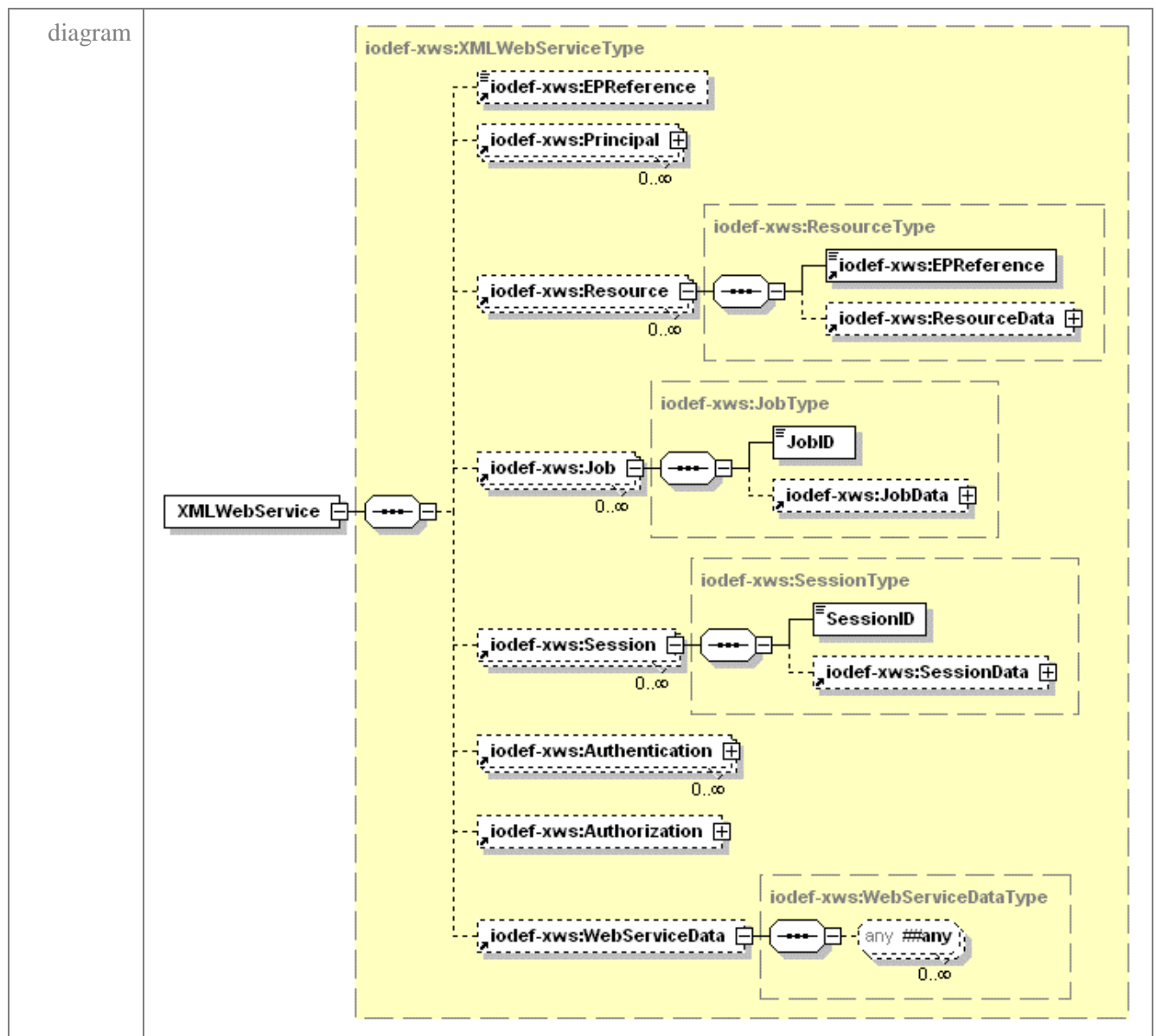
Describes and explains Grid specific IODEF elements. This is an update of the MJRA3.4 document [R2].

The proposed extension element XMLWebService and its components are described in detail in the XML Schema format below:

```

<!ELEMENT XMLWebService (EReference?, Principal*, Resource*, Job*,
Authentication*, Authorization?, WebServiceData?)>
  
```

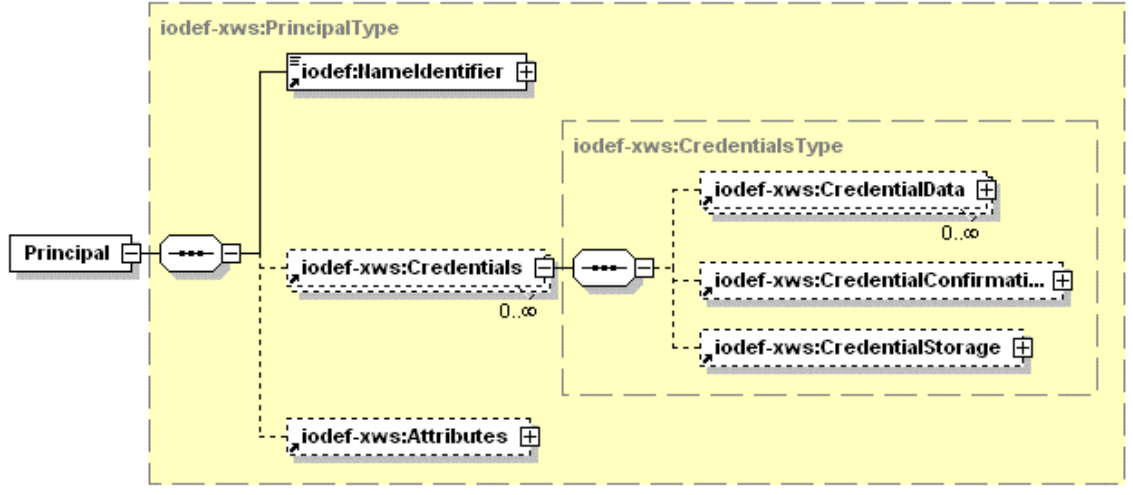
Element **XMLWebService** contains information about the Web Service or web application that was involved in the incident.



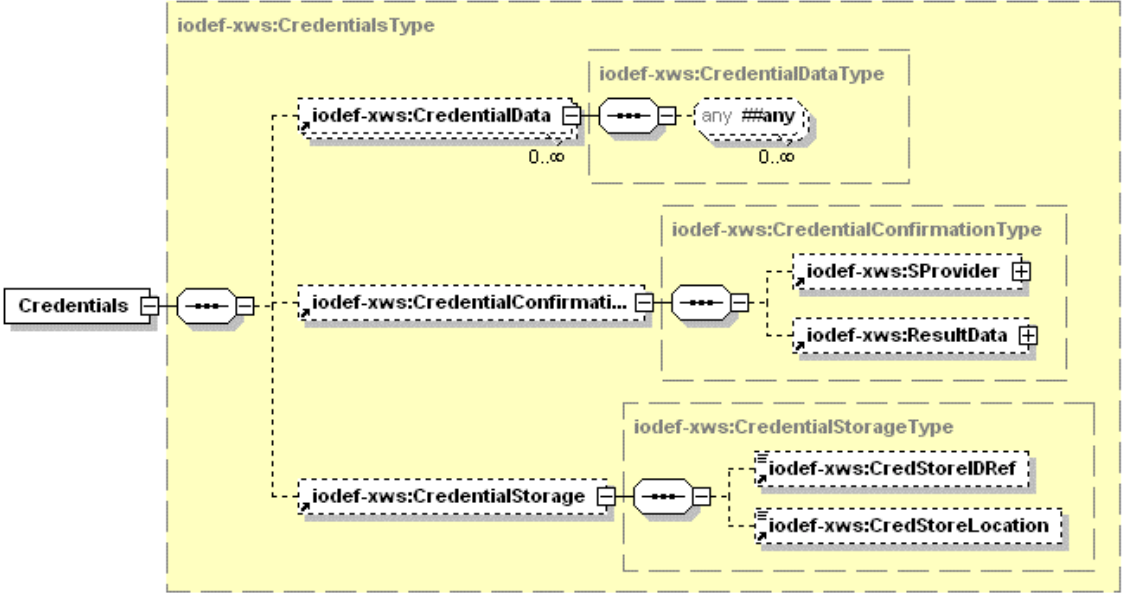
children	<p><b>EPReference</b> – End-Point Reference that uniquely identifies Web Service or Grid Service</p> <p><b>Principal</b> – entity participating in Web Service request or consumption</p> <p><b>Resource</b> – provides information about the Resource that was involved in the incident, suggested resources may be Computer Element (CE), Storage Element (SE), etc.</p> <p><b>ResourceData</b> – sub-element of the Resource containing arbitrary data about the resource, in particular, interface description or other information important for the Incident investigation</p> <p><b>Job/Session, JobID/ SessionID and JobData/SessionData</b> – describing Job (or Session) submitted to the service or resource that has relation to the incident</p> <p><b>Authentication</b> – contains information about the way the involved in the incident Principal was authenticated, including the case of failed authentication if this is classified as an incident</p> <p><b>Authorization</b> - contains information about the way the involved in the incident Principal was authorized to access the Web Service or perform a specific action, including the case of failed authorization if this is classified as a incident</p> <p><b>WebServiceData</b> – contains any additional information that describes the Web Service in details, including WSDL file or its components PortType, Binding, MessagePart; the element may also contain Request or Response messages that has relation to the incident</p>
Source XML Schema	<pre> &lt;xs:complexType name="XMLWebServiceType"&gt;   &lt;xs:sequence&gt;     &lt;xs:element ref="iodef-xws:EPReference" minOccurs="0"/&gt;     &lt;xs:element ref="iodef-xws:Principal" minOccurs="0" maxOccurs="unbounded"/&gt;     &lt;xs:element ref="iodef-xws:Resource" minOccurs="0" maxOccurs="unbounded"/&gt;     &lt;xs:element ref="iodef-xws:Job" minOccurs="0" maxOccurs="unbounded"/&gt;     &lt;xs:element ref="iodef-xws:Authentication" minOccurs="0" maxOccurs="unbounded"/&gt;     &lt;xs:element ref="iodef-xws:Authorization" minOccurs="0"/&gt;     &lt;xs:element ref="iodef-xws:WebServiceData" minOccurs="0"/&gt;   &lt;/xs:sequence&gt; &lt;/xs:complexType&gt; </pre>
Source XMLDTD	<pre> &lt;!ELEMENT XMLWebService (EPReference?, Principal*, Resource*, Job*, Authentication*, Authorization?, WebServiceData?)&gt; </pre>



Element **Principal** contains information about the entities participating in the Web/Grid Services interaction. It may be a user or other entity who owns the service, or on behalf of which the action or service were requested that were involved in the incident.

diagram	
children	<p><b>NameIdentifier</b> – contains name that uniquely identifies the Principal; the element suggests different formats including but not limited to email address, X.509NameQualifier, URN or other used locally.</p> <p><b>Credentials</b> – contains the credentials identifying the Principal and confirming the name contained in the NameIdentifier element; the Credentials element contains the sub-elements CredentialData, CredentialConfirmation and CredentialStorage</p> <p><b>Attributes</b> – contains the attributes that are associated with the subject and are important for the incident investigation; attributes that include Principal's roles, group or association, and also possible restrictions</p>
Source XML Schema	<pre> &lt;xs:complexType name="PrincipalType"&gt;   &lt;xs:sequence&gt;     &lt;xs:element ref="iodef:NameIdentifier"/&gt;     &lt;xs:element ref="iodef-xws:Credentials" minOccurs="0" maxOccurs="unbounded"/&gt;     &lt;xs:element ref="iodef-xws:Attributes" minOccurs="0"/&gt;   &lt;/xs:sequence&gt;   &lt;xs:attribute ref="iodef-xws:principalcat" default="other"/&gt; &lt;/xs:complexType&gt; </pre>
Source XML DTD	<pre> &lt;!ELEMENT Principal (NameIdentifier, Credentials*, Attributes?)&gt; </pre>

Element **Credentials** contains information about credentials related to principals involved in the incident.

<p>diagram</p>	
<p>children</p>	<p><b>CredentialData</b> – contains credential data in arbitrary format including X.509 Public Key Certificate (PKC), Attribute Certificate (AC), Proxy Certificate (Proxy), or XML assertions.</p> <p><b>CredentialConfirmation</b> – may contain information about the Authentication Service Provider and/or about the result</p> <p><b>CredentialStorage</b> – contains information about used credential storage including storage identification CredStoreIDRef and storage location CredStoreLocation</p> <p>Mandatory attribute of both Credentials and CredentialStorage elements is the storage status attribute <b>“status”</b> that indicates whether the credentials or storage are valid, protected, compromised, or quarantined.</p>
<p>Source XML Schema</p>	<pre> &lt;xs:complexType name="CredentialsType"&gt;   &lt;xs:sequence&gt;     &lt;xs:element ref="iodef-xws:CredentialData" minOccurs="0" maxOccurs="unbounded" /&gt;     &lt;xs:element ref="iodef-xws:CredentialConfirmation" minOccurs="0" /&gt;     &lt;xs:element ref="iodef-xws:CredentialStorage" minOccurs="0" /&gt;   &lt;/xs:sequence&gt;   &lt;xs:attribute ref="iodef:restriction" default="default" /&gt;   &lt;xs:attribute ref="iodef-xws:credstatus" use="required" /&gt; &lt;/xs:complexType&gt; </pre>
<p>Source XML DTD</p>	<pre> &lt;!ELEMENT Credentials (uid?, Name?, Certificate+, AdditionalData*)&gt; </pre>

Elements **Authentication** and **Authorization** contain information about AuthN/Z process and related data for entities or principals involved in the incident. These elements are also intended to provide a format for describing such security events as failed authentication or misused privileges.

diagram	
children	<p><b>AAContext</b> – the element containing context of the authentication and authorisation decision and may include provided credentials, attributes or other arbitrary data</p> <p><b>ContextData</b> – contains any arbitrary data that provide context for the authorisation or authentication decision</p> <p><b>SProvider</b> – contains information about the authorisation or authentication service providers that in particular provided access control service for the principal</p> <p><b>SResult</b> – contains information about the result of principal's authorisation or authentication including the case of failed authorization if its was classified as an incident; SResult contains the sub-elements Result and ResultData</p> <p><b>Result</b> – describes the result of the principal's authentication and authorisation by the SProvider in a free from or from the restricted enumerated list</p> <p><b>ResultData</b> – contains arbitrary data providing necessary background/context information supplementary to the result</p>
Source XML Schema	<pre>&lt;xs:complexType name="AuthenticationType"&gt;   &lt;xs:sequence&gt;     &lt;xs:element ref="ioodef-xws:AAContext" minOccurs="0"/&gt;     &lt;xs:element ref="ioodef-xws:SProvider" minOccurs="0"/&gt;     &lt;xs:element ref="ioodef-xws:SResult" minOccurs="0" maxOccurs="unbounded"/&gt;   &lt;/xs:sequence&gt;   &lt;xs:attribute ref="ioodef-xws:authnmethod" use="required"/&gt; &lt;/xs:complexType&gt;</pre>
Source	<pre>&lt;!ELEMENT Authentication (AAContext?, SProvider?, SResult*)&gt;</pre>

XML DTD	
------------	--

XML based nature of interactions in Web Services and Grids provides good integration basis between Incident reporting facilities and applications and their monitoring tools. Thus, original data in XML format can be placed into the extensibility **\*Data** elements that can adopt data formats from different namespaces than basic “iodef-xws” namespace.

The proposed extensions for description of the Grid Security Incident were discussed on IETF-INCH mailing list <inch@NIC.SURFNET.NL> [R8] and presented to the INCH WG for consideration.

Modelling of proposed extensions with the XML schema is presented at the IODEF Schema information site <http://www.uazone.org/demch/projects/iodef/> as IODEF version 0.42 [R9].

#### **4. SUMMARY**

The document presents updates and further development of Grid Security Incident data model and XML schema as extension to the IODEF incident description format that is used by CSIRTs for incident information exchange. Requirement for general Incident reporting format FINE adopted by the CSIRT community is reviewed for its possible use for Grid Security Incident reporting. The IODEF profile for XML Web Services and Grids is proposed based on general XML Web Services and Grid vulnerabilities analysis and basic services operational security model. It is perceived that XML based nature of interactions in Web Services and Grids can provide even better integration between Incident reporting facilities and applications and their monitoring tools than in network applications.

The information on IODEF profile for XML Web Services and Grid have been presented to the CSIRT community for discussion. However, in the framework of current EGEE Operational Security activity this stage is considered as final in the development of the proposed data model and exchange format. Further development may occur in case of practical implementation of the proposed format in CSIRT or Grid operational security practice.