Independent Submission
Request for Comments: 7444
Category: Informational
ISSN: 2070-1721

K. Zeilenga
A. Melnikov
Isode Limited

February 2015

Защитные метки в электронной почте Internet

Security Labels in Internet Email

Тезисы

В этом документе описано использование поля заголовка SIO-Label в электронной почте Internet для передачи информации о степени «секретности» сообщения в целом. Это поле может содержать текстовое (отображаемый маркер - display marking) и/или структурированное (защитная метка - security label) представление уровня секретности сообщения. Данный документ описывает также поле заголовка SIO-Label-History для записи изменений метки.

Статус документа

Данный документ не является спецификацией протокола Internet и публикуется с информационными целями.

Документ публикуется в серии RFC в качестве независимого от других ветвей RFC. Редактор (RFC Editor) публикует этот документ по своему усмотрению и не делает каких-либо заявлений о реализации или развертывании. Документ одобрен для публикации редактором RFC Editor и не претендует на роль какого-либо стандарта Internet (см. параграф 2 в RFC 5741).

Информация о текущем статусе этого документа, обнаруженных ошибках и способах обратной связи может быть найдена по ссылке http://www.rfc-editor.org/info/rfc7444.

Оглавление

1. Введение

Метки защиты (security label), иногда называемые метками конфиденциальности (confidentiality label), служат структурированным представлением уровня секретности части информации. Защитные метки могут использоваться вместе с разрешением (структурированная информация о людях или иных субъектах, которым разрешен доступ), а также правилами защиты в плане контроля доступа к каждой части информации. Например, почтовое сообщение может иметь метку EXAMPLE CONFIDENTIAL, требующую от получателя и отправителя наличия прав доступа к информации с меткой EXAMPLE CONFIDENTIAL. Защитные метки, разрешения и правила защиты рассмотрены в документе X.841 [X.841].

Отображаемые маркеры обеспечивают текстовое представление уровня конфиденциальности. Например, метка EXAMPLE CONFIDENTIAL может служить обозначением конфиденциальных сведений. Для генерации таких маркеров из защитных меток может использоваться политика безопасности. Предполагается, что в общем случае маркеры будут хорошо заметны при просмотре содержимого.

Предоставление полномочий на основе уровня конфиденциальности используется в сетях, работающих на основе некого набора правил классификации информации (например, сети правительственных или военных организаций). Стандартизованные форматы защитных меток, разрешений, правил защиты и связанных с этим моделей предоставления доступа обобщены для неправительственных организаций и могут применяться в подходящих случаях.

Метки защиты могут использоваться не только для управления правами доступа. В частности, они могут служить для передачи сведений об уровне конфиденциальности разных частей информации (например, при организации хранилищ).

В этом документе описан протокол передачи уровня конфиденциальности в сообщениях электронной почты [RFC5322]. В частности, документ описывает поле заголовка SIO-Label, содержащее метку защиты, отображаемые маркеры и цветовую маркировку. В документе также описано поле заголовка SIO-Label-History для записи сведений об изменении метки защиты.

Данный протокол основан на документе XEP-0258: Security Labels in XMPP [XEP258].

1.1. Взаимодействие с маркировкой в тексте

В средах, где требуется маркировка сообщений по уровню конфиденциальности, общепринятым является текстовое представление таких уровней в форме специальных маркеров (display marking) в теле сообщение и/или поле заголовка Subject (тема). Например, авторы зачастую получают сообщения вида:

```
To: author <author@example.com>;
From: Some One <someone@example.net>;
Subject: the subject (UNCLASSIFIED)

UNCLASSIFIED

Text of the message.

UNCLASSIFIED
```

Обычно при размещении в теле сообщения маркер помещается в качестве первой строки или нескольких строк. Такой вариант называют маркировкой FLOT[1]. Маркировка может окружаться дополнительным текстом, показывающим, что она обозначает уровень конфиденциальности сообщения. FLOT может также сопровождаться маркировкой LLOT[2]. В приведенном выше примере используются две строки FLOT и две строки LLOT (в обоих случаях маркер обозначается пустой строкой между ним и исходным содержимым).

При включении в поле Subject маркер обычно помещается перед исходным текстом темы сообщения и после него, иногда маркер помещается в скобки и/или отделяется от исходного текста пробелами.

Конкретный синтаксис и семантика встраиваемой в текст маркировки обычно задаются локально. Это осложняет взаимодействие внутри организации, желающей выполнять те или иные действия на базе маркировки, а также взаимодействие между сотрудничающими организациями, желающими с пользой совместно применять данные об уровне конфиденциальности.

Авторы предполагают продолжение широкого использования такой маркировки особенно в условиях отсутствия повсеместной поддержки стандартизованных полей заголовков, указывающих уровень конфиденциальности сообщения.

Авторы надеются, что наличие формальной спецификации поля заголовка будет способствовать упрощению взаимодействия между организациями.

1.2. Взаимодействие с существующими метками защиты

Используется множество нестандартных полей заголовков (например, X-X411) для передачи информации о конфиденциальности сообщений с использованием структурированной или текстовой формы.

Авторы надеются, что вместо применения существующих (нестандартных) полей заголовков с течением времени станут использоваться поля, описанные в данном документе.

1.3. Взаимодействие с ESS для S/MIME

Услуги ESS[3] для S/MIME (ESS) [RFC2634] обеспечивают, наряду с другими типами сервиса, подписи «для обеспечения целостности, невозможности отказа от авторства и [защищенного] связывания атрибутов (таких, как защитная метка) и исходным содержимым».

Хотя описанный в данном документе протокол может использоваться вместе с ESS, протокол прежде всего рассматривается, как альтернатива ESS.

Отмечено, что в ESS метка защиты относится к содержимому MIME [RFC2045], тогда как в данном протоколе метки относятся к сообщению в целом.

Отмечено также, что в ESS метки защищенным способом связываются с содержимым MIME за счет использования цифровых подписей. Данный протокол не предлагает услуг подписывания сообщений и, следовательно, не обеспечивает защищенной привязки метки к сообщению, защиту целостности и невозможность отказа от авторства.

Данный протокол предназначен для ситуаций/сред, где наличие цифровой подписи не требйется для обеспечения нужной защиты.

2. Используемые в документе соглашения

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с [RFC2119].

Формальная спецификация синтаксиса в этом документе использует представление ABNF[4], описанное в [RFC5234].

[1]First Line(s) of Text — первая строка (строки) текста.
[2]Last Line(s) of Text - последняя строка (строки) текста.
[3]Enhanced Security Services — услуги по улучшенной защите.
[4]Augmented Backus-Naur Form — расширенная форма Бэкуса-Наура.

Термин «представление base64» служит для обозначения кодирования Base 64, определенного в параграфе 4 [RFC4648]. Термин «BER-представление» служит для обозначения кодирования BER[1], определенного в [X.690].

3. Обзор

Пользовательский агент MUA[2], генерирующий сообщение, может при соответствующей настройке предлагать пользователю меню уровня конфиденциальности для выбора и последующего отображения маркеров, цвета фона и символов, а также параметров защитной метки, связанных с полем SIO-Label в заголовке сообщения.

Агенты подачи сообщений MSA[3], а также агеты передачи (MTA[4]) и доставки (MDA[5]) сообщений при соответствующей настройке будут использовать данные о конфиденциальности (или их отсутствие) при решении вопросов о приеме, пересылке или иных действиях с поданным сообщением. Эти агенты, далее обозначаемые, как сервисные агенты (SA[6]), могут при соответствующей настройке менять данные о конфиденциальности сообщения (изменять метку и/или маркер) эквивалентным представлением уровня конфиденциальности. Агентам SA, добавляющим, меняющим или удаляющим поле заголовка SIO-Label, **следует** сохранять информацию об этом в поле заголовка SIO-Label-History.

Принимающим агентам MUA, которые поддерживают данное расширение, **следует** при отображении сообщения выводить маркер (если он есть), полученный в поле заголовка SIO-Label или, в соответствии с политикой и конфигурацией, выполнять локальную маркировку, а также маркировку, созданную полученной меткой и требованиями регуляторов. Желательно также показывать эти маркеры в списке сообщений. В случае отображения полученного маркера его **следует** выводить с использованием цветов фона и текста, заданных полем заголовка. Если маркировка генерируется на основе полученной метки и требований регуляторов, маркер **следует** выводить с использованием цветов, заданных требованиями регуляторов.

Не предполагается принятие агентами MUA решений о предоставлении доступа на основе значений поля SIO-Label, MUA могут использовать предоставленную информацию об уровне конфиденциальности (или ее отсутствие) для определения действий по отношению к принятому сообщению. Например, MUA могут организовать хранение сообщений с учетом содержимого описываемого поля.

4. Поле заголовка SIO-Label

Поле заголовка называется SIO-Label и включает набор пар «ключ-значение», каждая из которых рассматривается, как параметр.

Формальный синтаксис поля представлен ниже:

```
sio-label = "SIO-Label:" [FWS] sio-label-parm-seq [FWS] CRLF

sio-label-parm-seq = sio-label-parm [ [FWS] ";" [FWS] sio-label-parm-seq ]

sio-label-parm = parameter
```

Параметры определены в [RFC2231], FWS — в [RFC5322], а добавление CRLF — в [RFC5234]. Отметим, что параметры, определенные в [RFC2231], основаны на формате ABNF [RFC0822], которые неявно допускает в некоторых случаях включение пробельных символов. В частности, такие символы неявно разрешены в параметрах, непосредственно предшествующих и следующих за знаком равенства (=). Отметим также, что [RFC2231] разрешает заключенные в кавычки строки (для создания параметров) значительной длины для строк в кодировках, отличных от US-ASCII, и других подобных случаев. Разработчикам следует обратиться за подробностями к упомянутым спецификациям.

Параметр marking (маркер) представляет собой отображаемую строку для использования в реализациях, в которых невозможно или нежелательно следование требованиям регуляторов в части генерации маркировки. Обычно этот параметр **следует** включать в поля SIO-Label. Его отсутствие допустимо лишь в тех случаях, когда агент SA при генерации маркировки опирается на другие SA.

Цветовые параметры (fgcolor — цвет текста и bgcolor — цвет фона) являются маркерами, определяющими выбор цветов для отображения текста и фона, соответственно. Их значения могут указываться в шестнадцатеричном представлении RGB (например, "#ff0000") или в форме именованных цветов CSS[7](например, red — красный), перечисленных ниже (16 цветов HTML4 и orange - оранжевый) [CSS3-Color]. По умолчанию применяется черный фон и белые символы. При отсутствии параметра marking **нужно** опускать также параметры fgcolor и bgcolor. Формат представления HEXDIG определен в [RFC5234].

Формальный синтаксис показан ниже:

```
color = hex-color / named-color

hex-color = "#" 6HEXDIG    ; Шестнадцатеричное представление RGB

named-color =
           "aqua" /
           "black" /
           "blue" /
           "fuschia" /
           "gray" /
           "green" /
```

[1]Basic Encoding Rules — базовые правила кодирования.
[2]Mail User Agent – пользовательский почтовый агент.
[3]Mail Submission Agent.
[4]Mail Transfer Agent.
[5]Mail Delivery Agent.
[6]Service Agent.
[7]Cascading Style Sheet.

```
                "lime" /
                "maroon" /
                "navy" /
                "olive" /
                "purple" /
                "red" /
                "silver" /
                "teal" /
                "white" /
                "yellow" /
                "orange" ; именованные цвета
```

Параметр type (тип) представляет собой заключенную в кавычки строку, содержащую текст «:ess», «:x411», «:xml» или URI [RFC3986], определяющие тип и представление параметра label (метка). Метка представляет собой заключенную в кавычки строку. При наличии параметра label **нужно** включать и параметр type. При управлении доступом (authorization) на основе данных об уровне конфиденциальности отсутствие параметров type и label показывает, что сообщение обрабатывает в соответствии с принятыми по умолчанию правилами (например, при отсутствии SIO-Label).

Строка «:ess» говорит, что параметр label представляет собой форму base64 для BER-кодирования защитной метки ESS [RFC2634].

Пример метки ESS:

```
SIO-Label: marking="EXAMPLE CONFIDENTIAL";
    fgcolor=black; bgcolor=red;
    type=":ess"; label="MQYGASkCAQM="
```

Строка «:x411» показывает, что параметр label представляет собой форму base64 для BER-кодирования защитной метки X.411 [X.411].

Пример метки X.411:

```
SIO-Label: marking="EXAMPLE CONFIDENTIAL";
    fgcolor=black; bgcolor=red;
    type=":x411"; label="MQYGASkCAQM="
```

Строка «:xml» говорит, что параметр label содержит форму base64 для защитной метки, представленной с применением [XML]. Пролог XML **следует** опускать, если иного не требуется (например, при кодировке, отличной от UTF-8). Специфика представления защитной метки задается корневым элементом имени и его пространством имен.

Пример метки XML:

```
SIO-Label: marking="EXAMPLE CONFIDENTIAL";
    fgcolor=black; bgcolor=red;
    type=":xml";
    label*0="PFNlY0xhYmVsIHhtbG5zPSJodHRwOi8vZXhhbX";
    label*1="BsZS5jb20vc2VjLWxhYmVsLzAiPjxQb2xpY3lJ";
    label*2="ZGVudGlmaWVyIFVSST0idXJuOm9pZDoxLjEiLz";
    label*3="48Q2xhc3NpZmljYXRpb24+MzwvQ2xhc3NpZmlj";
    label*4="YXRpb24+PC9TZWNMYWJlbD4=";
```

где метка XML с новыми строками и пробельными символами для удобочитаемости имеет вид:

```
<SecLabel xmlns="http://example.com/sec-label/0">
    <PolicyIdentifier URI="urn:oid:1.1"/>
    <Classification>3</Classification>
</SecLabel>
```

Форматы :ess и :x411 **следует** использовать для представления защитных меток ESS и X.411, соответственно, вместо прямого XML-представления этих форматов.

В минимальный вариант поля **нужно** включать параметр marking и оба параметра type и label.

Это поле может быть расширено путем включения дополнительных параметров в новых документах, дополняющих (или заменяющих) данный. В реализациях **следует** игнорировать нераспознанные дополнительные параметры. Эти рекомендации не являются обязательными и позволяют агентам обрабатывать сообщения с нераспознанными параметрами в поле SIO-Label отлично от сообщений, где SIO-Label не содержит неизвестных параметров.

В заголовок каждого сообщения **нужно** включать не более одного поля SIO-Label.

Расширенный пример:

```
SIO-Label: marking*=us-ascii'en'EXAMPLE%20CONFIDENTIAL;
    fgcolor = black ; bgcolor = red ;
    type=":ess"; label*0="MQYG";
    label*1="ASkCAQM="
```

Этот пример эквивалентен приведенному выше примеру метки ESS.

5. Поле заголовка SIO-Label-History

Любой агент SA **может** записывать изменения метки в поле SIO-Label-History. Это поле предназначено для трассировки изменений (и только для нее). Например, оно может служить для записи сведений о добавлении, изменении или удалении метки сервисным агентом. Поле может также применяться в иных ситуациях. Например, шлюз, транслирующий сообщения X.400 в электронную почту RFC 5322, может использовать это поле для записи внесенных при трансляции изменений метки.

Поле SIO-Label-History рассматривается, как трассировочное, в соответствии с определением в параграфе 3.6.7 [RFC5322].

Формальный синтаксис поля SIO-Label-History совпадает с синтаксисом SIO-Label, но содержит дополнительные параметры:

- change — одно из значений add, replace, delete;
- changed-by — строка, идентифицирующая агент (в общем случае, полное доменное имя агента);
- changed-at — дата и время внесения изменений в формате [RFC5322];
- changed-comment — строка комментариев;
- marking, fgcolor, bgcolor, type, label — значения параметров метки до внесения изменений в SIO-Label с использованием синтаксиса параметров, определенного для параметров SIO-Label (для операций add эти параметры не указываются);
- new-marking, new-fgcolor, new-bgcolor, new-type, new-label — значения параметров метки после внесения изменений с использованием синтаксиса, определенного для параметров SIO-Label (для операции delete эти параметры не указываются).

В минимальное поле **нужно** включать параметры change, changed-by, changed-at.

Это поле может быть расширено путем включения дополнительных параметров в новых документах, дополняющих (или заменяющих) данный.

Каждое сообщение может содержать множество полей SIO-Label-History. Все поля SIO-Label-History следует размещать непосредственно вслед за полем SIO-Label в виде одной группы. Добавляемое поле SIO-Label-History следует размещать непосредственно перед всеми имеющимися полями SIO-Label-History.

Примеры SIO Label History вида Add, Modify, Delete:

```
SIO-Label-History: marking="EXAMPLE CONFIDENTIAL";
    fgcolor=black; bgcolor=red;
    type=":xml";
    label*0="PFNlY0xhYmVsIHhtbG5zPSJodHRwOi8vZXhhbX";
    label*1="BsZS5jb20vc2VjLWxhYmVsLzAiPjxQb2xpY3lJ";
    label*2="ZGVudGlmaWVyIFVSST0idXJuOm9pZDoxLjEiLz";
    label*3="48Q2xhc3NpZmljYXRpb24+MzwvQ2xhc3NpZmlj";
    label*4="YXRpb24+PC9TZWNMYWJlbD4=";
    change=delete;
    changed-by="delete.example.com";
    changed-at="18 Feb 2013 9:24 PDT";
    changed-comment="delete"
SIO-Label-History: marking="EXAMPLE CONFIDENTIAL";
    fgcolor=black; bgcolor=red;
    type=":ess"; label="MQYGASkCAQM=";
    new-marking="EXAMPLE CONFIDENTIAL";
    new-fgcolor=black; new-bgcolor=red;
    new-type=":xml";
    new-label*0="PFNlY0xhYmVsIHhtbG5zPSJodHRwOi8vZXhhbX";
    new-label*1="BsZS5jb20vc2VjLWxhYmVsLzAiPjxQb2xpY3lJ";
    new-label*2="ZGVudGlmaWVyIFVSST0idXJuOm9pZDoxLjEiLz";
    new-label*3="48Q2xhc3NpZmljYXRpb24+MzwvQ2xhc3NpZmlj";
    new-label*4="YXRpb24+PC9TZWNMYWJlbD4=";
    change=replace;
    changed-by="modify.example.net";
    changed-at="18 Feb 2013 8:24 PDT";
    changed-comment="replaced with XML variant"
SIO-Label-History: new-marking="EXAMPLE CONFIDENTIAL";
    new-fgcolor=black; new-bgcolor=red;
    new-type=":ess"; new-label="MQYGASkCAQM=";
    change=add;
    changed-by="add.example.net";
    changed-at="18 Feb 2013 7:24 PDT";
    changed-comment="added label"
```

6. Согласование с IANA

Поля SIO-Label и SIO-Label-History зарегистрированы в реестре Provisional Message Header Field Registryв соответствии с [RFC3864].

Имя поля заголовка: SIO-Label

Применим к протоколам: mail [RFC5322]

Статус: provisional

Автор/контролер изменений: Kurt Zeilenga (kurt.zeilenga@isode.com)

Спецификация: RFC 7444

Имя поля заголовка: SIO-Label-History

Применим к протоколам: mail [RFC5322]

Статус: provisional

Автор/контролер изменений: Kurt Zeilenga (kurt.zeilenga@isode.com)

Спецификация: RFC 7444

7. Вопросы безопасности

Конфиденциальную информацию следует защищать подобающим образом (независимо от наличия метки). Для сообщений электронной почты обычно подходит аутентификация передающей стороной приемной стороны для организации защиты на транспортном уровне, включая защиту целостности и конфиденциальности данных. Когда приемная сторона решает вопрос предоставления доступа на основе представления передающей стороны, включая ее самоидентификацию, этого обычно бывает достаточно для аутентификации передающей стороны.

Данный документ обеспечивает способ обозначения уровня конфиденциальности сообщений электронной почты. Указание уровня секретности сообщения в общем случае не повышает этот уровень, однако само это указание может рассматриваться как конфиденциальная (секретная) информация. Например, маркировка BLACK PROJECT RESTRICTED может раскрыть существование секретного проекта.

Поле SIO-Label показывает уровень конфиденциальности сообщения в целом, включая его заголовок и содержимое. Данный документ не описывает способов указания уровня конфиденциальности отдельных частей сообщения (например, разного уровня конфиденциальности разных частей MIME, содержащихся в сообщении). Преимуществами предложенной в документе модели являются простота и легкость применения (единственное указание уровня конфиденциальности) по сравнению со сложностью и трудностью независимой маркировки отдельных частей.

Указанный уровень конфиденциальности может использоваться для определения способов обработки сообщений. Например, значение поля SIO-Label (или его отсутствие) можно использовать для решения о пересылке сообщения тому или иному адресату, а в случае пересылки — для определения минимальных требований по защите на пути пересылки. Механизм определения способов обработки сообщений на основе маркировки по уровню конфиденциальности выходит за пределы настоящего документа.

Реальное содержимое сообщения по уровню конфиденциальности может отличаться от указанного в заголовке уровня. Агентам следует избегать понижения уровня защиты при обмене сообщениями на основе указанного в заголовке уровня конфиденциальности.

Данный протокол сам по себе не обеспечивает услуг подписания сообщений типа тех, которые применяются для защиты целостности, невозможности отказа от авторства и привязки атрибутов (таких, как метки защиты в сообщениях). Хотя этот протокол может использоваться вместе со службами подписи, данный документ не детализирует такие применения.

Предполагается, что защитные метки и отображаемые маркеры указывают одинаковый уровень конфиденциальности, однако данная спецификация не требует такого совпадения. Например, MUA может представить сообщение, в котором метка защиты указывает некий уровень конфиденциальности, а отображаемый маркер показывает иной уровень, что может вызвать в агентах SA проблемы, связанные с неподобающей обработкой сообщения. Обычно для каждого SA приемлемо использование значений SIO-Label для проверки совпадения уровней конфиденциальности в метке защиты и отображаемом маркере с принятием подобающих мер (например, отказ в приеме) в случае расхождения.

Этот документ также обеспечивает средство фиксации изменения метки в сообщении. Это средство предназначено исключительно для трассировки. Следует отметить, что поле SIO-Label-History может включать конфиденциальную информацию и, следовательно, может удаляться из сообщения в случаях возможности раскрытия информации на основании содержащихся в этом поле данных.

8. Литература

8.1. Нормативные документы

[CSS3-Color] Celik, T. and C. Lilley, "CSS3 Color Module", W3C Candidate Recommendation CR-css3-color-20030514, May 2003, <http://www.w3.org/TR/2003/CR-css3-color-20030514>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, <http://www.rfc-editor.org/info/rfc2119> (перевод).

[RFC2231] Freed, N. and K. Moore, "MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations", RFC 2231, November 1997, <http://www.rfc-editor.org/info/rfc2231>.

[RFC2634] Hoffman, P., Ed., "Enhanced Security Services for S/MIME", RFC 2634, June 1999, <http://www.rfc-editor.org/info/rfc2634>.

[RFC3864] Klyne, G., Nottingham, M., and J. Mogul, "Registration Procedures for Message Header Fields", BCP 90, RFC 3864, September 2004, <http://www.rfc-editor.org/info/rfc3864>.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005, <http://www.rfc-editor.org/info/rfc3986>.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, October 2006, <http://www.rfc-editor.org/info/rfc4648>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008, <http://www.rfc-editor.org/info/rfc5234> (перевод).

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, October 2008, <http://www.rfc-editor.org/info/rfc5322> (перевод).

[X.411] ITU-T, "Message Handling Systems (MHS) — Message Transfer System: Abstract Service Definition and Procedures", ITU-T Recommendation X.411, June 1999.

[X.690] ITU-T, "ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU-T Recommendation X.690, November 2008.

[XML] Bray, T., Paoli, J., Sperberg-McQueen, C., Maler, E., and F. Yergeau, "Extensible Markup Language (XML) 1.0 (Fifth Edition)", W3C Recommendation REC-xml-20081126, November 2008, <http://www.w3.org/TR/2008/REC-xml-20081126>.

8.2. Дополнительная литература

[RFC0822] Crocker, D., "STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES", STD 11, RFC 822, August 1982, <http://www.rfc-editor.org/info/rfc822>.

[RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996, <http://www.rfc-editor.org/info/rfc2045>.

[X.841] ITU-T, "Security information objects for access control", ITU-T Recommendation X.841, October 2000.

[XEP258] Zeilenga, K., "XEP-0258: Security Labels in XMPP", XEP XMPP Extension Protocols, April 2013.

Благодарности

Авторы благодарят членов сообщества, включая Dave Cridland, Brad Hards, Russ Housley, Steve Kille, Graeme Lunt, Alan Ross, Jim Schaad, David Wilson за просмотр документа, комментарии и предоставленные тексты.

Адреса авторов

Kurt Zeilenga

Isode Limited

EMail: Kurt.Zeilenga@isode.com

Alexey Melnikov

Isode Limited

14 Castle Mews

Hampton, Middlesex TW12 2NP

United Kingdom

EMail: Alexey.Melnikov@isode.com

Перевод на русский язык

Николай Малых

nmalykh@protocols.ru