Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 26, 2015

J. Davin
June 24, 2015

Email Exchange of Secondary School Transcripts
draft-davin-eesst-03

Abstract

A common format simplifies exchange of secondary school academic transcripts via electronic mail. Extant standards are applied to prevent unauthorized alteration of transcript content and to deliver transcripts directly and securely from each student to his or her chosen recipients. By eliminating third-party intervention and surveillance, the defined protocol better protects student privacy and independence than does current practice.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79. This document may not be modified, and derivative works of it may not be created, except to format it for publication as an RFC or to translate it into languages other than English.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/[1].

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as “work in progress”.

This Internet-Draft will expire on December 26, 2015.

Copyright Notice

[1] http://datatracker.ietf.org/drafts/current/
[2] http://trustee.ietf.org/license-info

Table of Contents

1. Introduction

Traditional, paper-based communication of individual student records protects the rights and interests of all stakeholders -- the secondary school officials who curate student records, the students who are both the subjects and distributors of their own individual records, and the college admission officers, prospective employers, and others who, with the permission of individual students, receive and review such records. In the traditional process, when a graduating student applies for employment or admission to an institution of higher learning, she asks the guidance counselor at her secondary school for a transcript of her academic achievements to support her application. In response, the guidance counselor prepares a paper record of that student's achievements and presents it to her so that she might forward that transcript to whomever she pleased. In order to prevent forgery of academic transcripts, the paper record presented to the student often includes various marks of its authenticity, such as an imprint of the school seal or the signature of an authorized school official. In order to prevent unauthorized alteration of transcript content, the prepared document is presented to the student inside a sealed postal envelope which cannot easily be opened without detection -- sometimes aided by tamper-proof tape, signed envelope flaps, or even imprinted wax seals. The integrity of the envelope's physical seal assures the recipient that its contents have not been altered in transit; seals and signatures affixed to the enclosed document assure the recipient of the transcript's legitimacy. The student's privacy is assured by her ability to forward the sealed transcript to whomever she pleases without the knowledge of or further consultation with the school.

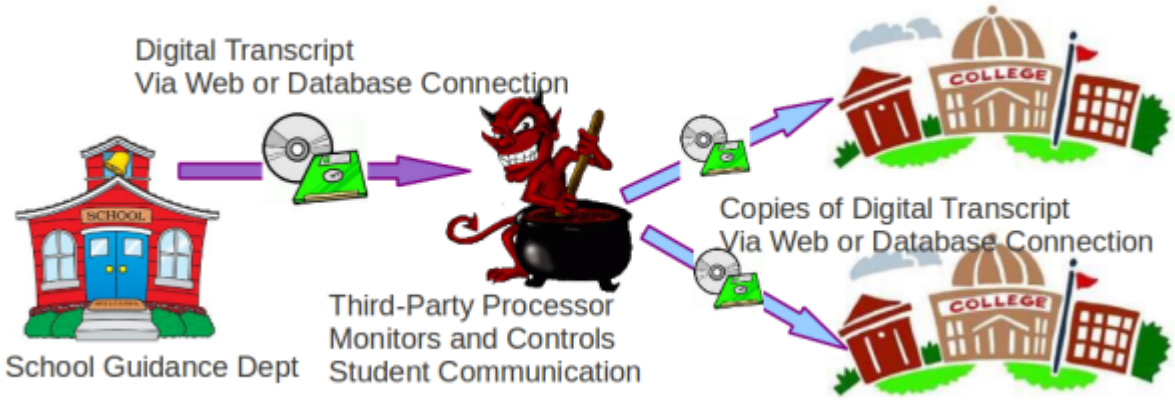

Figure 1: Corrupted Model for Exchanging Secondary School Transcripts

While the traditional process of distributing academic transcripts admirably protects student privacy and prerogatives, that process also requires manual effort from the school staff for the preparation of each transcript. On the premise of reducing that effort, some school officials have gratuitously misapplied technology in a way that guts student privacy and effectively excludes students from their own business. Figure 1 illustrates an increasingly common aberration. Rather than adopting standardized, readily available technology to protect the integrity of transmitted student data -- as it had once been protected by their own signatures on sealed envelopes -- school officials interpose themselves (or their agents) between students and transcript recipients, claiming falsely that no other approach adequately assures the confidentiality, origin, and integrity of transcript content or the reliability of transcript transmission. By introducing the role of "third-party processor" in Figure 1, educators disrupt what should be private, bilateral relationships between students and their chosen correspondents, implicitly denying the legitimacy of any technical means by which a student might manage and secure his/her own communication.

By coercing students into a false choice between surrendering their privacy or accepting the limitations of a neglected, largely manual system, educators and allied service providers gain significant new benefits at student expense. Among these benefits is the creation of an otherwise unneeded educational services industry

to mediate communication between students and transcript recipients -- communication which, by the most natural operation of the Internet, would otherwise be end-to-end. A second consequence of coerced mediation is that the mediators gain unfettered control over school records that would otherwise be private and often protected by law. A third consequence of coerced mediation is that mediators can harvest candid data on student behavior outside the secondary school domain. Even the most basic information about college and employment applications, successful or not, individual or in the aggregate, can have significant value for secondary school officials, college administrators, employers, and general marketing professionals. Moreover, although such data is historically private, it is also more valuable and legally less well protected than internal secondary school records.

Mediated transcript distribution vitiates student privacy while endowing school bureaucrats and their confederates with undeserved privilege, but these political concessions are utterly unnecessary to automated transcript distribution. As suggested by Figure 2, the political concessions intrinsic to mediated transcript exchange can be largely eliminated by the most straightforward automation of the traditional transcript process.

This memo specifies a common format for exchanging secondary school academic transcripts via electronic mail. Because the defined format supports digital signature of transcripts by their originator, a student cannot fabricate or alter transcript information provided by school officials. Because the described format supports encrypted transmission of school transcripts, the distribution of each student's information can remain private and under his or her control. Because the format supports asymmetric cryptography, the origin and integrity of received transcripts can be verified independently by the recipient; confidential content can be independently recovered by an intended recipient while remaining protected from unauthorized access. Because the Internet email protocol provides fail-safe delivery, transcripts are reliably delivered to their intended recipients, and the sending student is directly notified of any exceptions. No centralized, trusted authority is needed to mediate communication between students, transcript originators, or transcript recipients. Thus, a student's need for an authoritative record of his education cannot be exploited to restrict or monitor his/her free and private interactions with colleges, employers, or others. Students can reclaim control over their own personal information and their relationships with prospective employers and admissions officers; students can prevent surreptitious harvesting of information about their affairs. Last but not least, specialized software is not required by most participants in the school transcript exchange protocol: the needs of all students and many transcript recipients can be met by existing, standards-based, secure email clients.

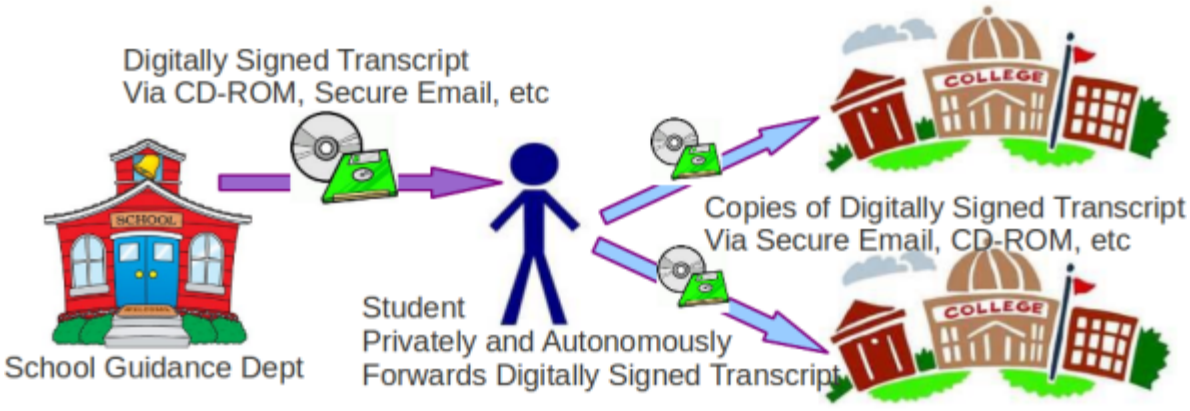

Figure 2: Traditional Model for Exchanging Secondary School Transcripts

The acronym EESST (Email Exchange of Secondary School Transcripts) names the format and methods defined here for securely conveying student academic records under student control. Requirements for implementors of this specification are expressed here using a keyword vocabulary [1] that is widely understood within the Internet community.

2. Design Motivation

Implicit in any protocol definition is some assignment of functions to the various protocol participants. When those participants are administratively independent one from another, binding assignments of protocol function -- which might otherwise seem purely technical choices -- are politically significant. For the sake of transparency, this protocol specification explicitly reckons the political consequences of its implicit design choices.

Preparation and delivery of secondary school transcripts most affects the interests of individual students. After all, the process is entirely motivated by a student's need to certify his or her personal academic achievements as evidence of merit for employment, higher education, or other social advancement or reward. Accordingly, individual student needs properly dominate the design of a common system for transcript exchange. Because a secondary school transcript certifies a student's personal merit, students need transcript documents that are credible to recipients -- for which the origin and integrity of transcript content is assured. Because a school transcript records personal information about an individual student, student privacy is paramount: control of transcript distribution must be closely held by the individual student, and each student must be able to protect the confidentiality of his or her transcript in transit.

Communication of transcript content between originator, student, and ultimate recipient is most secure only if that communication is end-to-end. While the end-to-end argument [11] is fundamental to the design of the Internet, it is also critical to the design of secure communication protocols (see Section 6.2, page 6 in RFC 1958 [12]). In contrast, securely communicating student information to a centralized (and otherwise uninvolved) third party clearly degrades student privacy and increases cost. Claims to the contrary are at best logically absurd and at worst darkly motivated.

After students, transcript handling must address the interests of transcript recipients, which may include college admission officers, prospective employers, scholarship foundations. Recipients must be able to evaluate the origin and integrity of received transcript documents easily and independently. Secondarily, recipients may benefit from mechanical extraction and summary of transcript content to support their own internal decision processes.

Finally, common transcript handling must address the needs of the transcript originator -- typically a secondary school guidance counselor or other school official. An originator's legitimate interests are reducing the cost of preparing transcript documents and meeting any legal or moral obligations to protect student privacy. Insofar as the very notion of electronic school transcripts implies their automated preparation by computers, dramatic cost reductions over traditional manual processes are also implicit. An originator's obligation to protect student privacy is most elegantly and inexpensively met by simply not conveying transcript information about a particular student to anyone other than that student.

A protocol by which students must request transcript distributions addresses no actual student need but, rather, only the legal needs of third-parties seeking to intervene in otherwise private communications. The additional effort of formal transcript requests is needed only when a mediating third party is involved, because, in many jurisdictions, sharing personal information with the third-party legally requires student consent, and an electronic transcript request may be conveniently construed as implicit consent. Moreover, a formal transcript request-response protocol is not needed to document delivery of a transcript to its intended recipient. When the student, rather than a third-party, directly conveys his/her transcript to a chosen recipient, that student has the greatest interest in successful communication, can observe any communication failures first-hand, and take corrective action if needed. Familiar, standardized protocols provide unambiguous feedback to the student about successful transcript delivery. The SMTP protocol, in particular, is defined and implemented to be failsafe, as described in section 4.1.1.4, page 33, of its specification [14]:

> Receipt of the end of mail data indication requires the server to process the stored mail transaction information. This processing consumes the information in the reverse-path buffer, the forward-path buffer, and the mail data buffer, and on the completion of this command these buffers are cleared. If the processing is successful, the receiver MUST send an OK reply. If the processing fails the receiver MUST send a failure reply. The SMTP model does not allow for partial failures at this point: either the message is accepted by the server for delivery and a positive response is returned or it is not accepted and a failure

reply is returned. In sending a positive completion reply to the end of data indication, the receiver takes full responsibility for the message (see section 6.1). Errors that are diagnosed subsequently MUST be reported in a mail message, as discussed in section 4.4.

3. Protocol Overview

Extant, standardized technology simplifies the process of preparing and distributing secondary school transcripts. Using a computerized procedure, a secondary school administrator prepares a digital transcript document that records the academic achievements of a particular student and presents that document to that student. Using postal delivery, secure email, or other method, the student conveys digital copies of the prepared transcript to recipients of his or her choice. Using a computerized procedure, each recipient may independently verify that the received transcript has not been forged or altered in transit. Because the received transcript is digital, each recipient may use computerized procedures to extract and summarize transcript content for local review and processing.

Preparing and delivering a secondary school transcript entails interaction among three kinds of participant -- transcript originator, student, and transcript recipient -- each of whom performs a distinct functional role. Interactions between each kind of participant are proscribed below.

3.1 Student and Originator

A transcript originator assembles and digitally signs academic transcripts that document the achievements of individual students in a secondary school. The role of transcript originator is frequently filled by the director of a high school guidance department or other secondary school official. At fixed times throughout the school year, using then-current information from a student database, the guidance director executes a computer program that, for each relevant student, automatically creates an individual transcript report and digitally signs that report on the director's behalf. The format of each signed transcript document is defined in Section 5 below.

The principal responsibilities of a transcript originator are:

1. Generate an OpenPGP keypair that can be used to sign school transcripts.
2. Create and securely store a key revocation certificate for the signing keypair for possible future use should it be compromised.
3. Publish on the world wide web the public component of the transcript signing keypair, together with its OpenPGP fingerprint.
4. Securely store the private component of the signing keypair and protect its use with a judiciously chosen passphrase known only to the transcript originator.
5. Use the signing keypair to create and digitally sign transcripts for individual students.
6. Present each signed transcript confidentially to the individual student to which it pertains.

Once generated by the transcript originator, each transcript is conveyed to the relevant student using any means that protects the confidentiality of individual student data. For example, a digital transcript may be written to a CD-ROM storage disk and presented to the relevant student when he comes to school. Alternatively, that same CD-ROM could be sealed in an envelope and sent to the student via postal delivery. A student could present a USB flash drive in person at the school guidance office, and her digital transcript could be copied onto that drive. A digital school transcript could also be presented to the relevant student as a MIME attachment to an email message that is encrypted according to the OpenPGP standard. When email is used to convey school transcripts to students, formatting such messages as specified in Section 6 below will foster security and interoperability.

After a student receives his/her transcript from its originator, that student is solely responsible for conveying that transcript to any recipients of his/her choosing, as described in Section 3.2 below.

3.1.1 Transcript Requests

For several reasons, how students request generation of an academic transcript from their secondary school is a local matter that need not and ought not be addressed here.

First, the volume of requests for transcripts is likely to be relatively low, because transcripts can be pre-issued to most students (e.g., graduating seniors) who are likely to need them. When transcripts are digital and easily

duplicated by the student, there is no need to generate a new transcript document for each desired recipient. Accordingly, most transcript generation is driven not by student requests but rather by content updates arising from the predictable passing of marking periods or academic sessions throughout the school year. Thus, explicit requests for transcript generation will be the exception rather than the rule -- from students who have lost a previously issued transcript, or students leaving the school prior to their graduation.

Second, an historical motivation for formalizing transcript requests has been to satisfy the school's legal obligation to protect student privacy. In many legal jurisdictions, school officials are required to seek student authorization for releasing information to a third party. Elaborate procedures for requesting transcripts are attempts to codify or automate that authorization process. However, because, under the procedure defined here, each student's information is provided only to that student, no authorization for releasing information to a third party is required.

Third, a codified transcript request protocol affords almost no benefit beyond enabling third party processors to assume the role of transcript originator and/or distributor. Students need no formal "acknowledgment" of their transcript requests: the transcript itself serves that purpose. Because a digital transcript is easily generated by an automated procedure, there is no benefit to returning a request acknowledgment rather than the document actually requested. The primary goal of this protocol design is to strengthen student privacy and agency by eliminating third-party intrusion into what would otherwise be private, bilateral interactions between a student and his school. To codify transcript requests is to undercut directly that fundamental purpose, while gratuitously restricting local interactions between student and school.

When each student -- rather than a school official or mediating third-party -- exercises principal control of distributing his or her own transcript information, any need for transcript requests is largely obviated. Thus, exchanging and processing such requests is properly a local matter and not further addressed here.

3.2 Student and Recipient

When a student is asked (e.g., by a college admissions office or prospective employer) to provide an official transcript of his or her academic achievements, that student may send to the requesting party a copy of the digitally signed transcript document that he has previously received from his secondary school. In this context, the party requesting that the student send a transcript is called a transcript recipient. Because it is the student who conveys his own transcript information, he or she unambiguously controls the set of recipients, and neither the secondary school nor any third party is responsible for or privy to the identities of his correspondents. Similarly, the student is responsible for assuring the privacy of his or her personal information as he conveys it to these recipients.

The student may convey his transcript to his chosen recipient using any mutually agreeable strategy. For example, he may print a copy of his transcript onto a postcard and send it via postal delivery. This strategy does not strongly protect the confidentiality of the student's information in transit, nor does this strategy allow the recipient to automate verification or other processing of the received transcript information. Sending a paper transcript sealed in a postal envelope better protects student confidentiality, but similarly restricts the recipient's ability to verify or process transcript contents. By copying his digital transcript onto a CD-ROM storage disk and sending that disk, sealed in a postal envelope, via surface mail, the recipient can automatically verify and process the transcript content, although protection of student confidentiality in transit might be stronger.

Alternatively, a student could send a copy of the digital transcript provided by his secondary school merely by attaching the relevant computer file to an email message addressed to the recipient. If the student completely trusts the end-to-end email transmission path from himself to his intended recipient (e.g., if student and recipient are connected by a common, private network), then the student could send his transcript in a plaintext email; otherwise, the student SHOULD encrypt the email contents to protect his privacy during transmission.

If a student chooses to convey his/her school transcript to a transcript recipient via electronic mail, then the principal responsibilities of that student are:

1. Create a personal email account and associated email address from which transmissions of the student's signed school transcript may be sent.

2. For each potential recipient of the student's signed school transcript, discover and record the email address and the public OpenPGP key published by that transcript recipient.
3. Import the OpenPGP public key for each chosen recipient into the local OpenPGP key database.
4. Use an email client application that implements the OpenPGP / MIME standard [13] in order to encrypt and transmit a copy of the signed school transcript to each chosen recipient.

Using common formats and methods to convey transcript content protects students while also simplifying processing for transcript recipients. Representing a transcript as specified in Section 5 below and using the transmission formats specified in Section 6 affords privacy and autonomy to students. By using these formats, recipients may independently verify the origin and integrity of the transcript information that students provide. Common transcript representation also allows recipients to automate the storage, analysis, and review of received transcripts.

However, a student cannot use the format specified here to convey his/her transcript to a chosen recipient unless that recipient is prepared to participate in the exchange. The principal responsibilities of a transcript recipient are:

1. Generate an OpenPGP keypair that can be used to encrypt student transmissions of signed school transcripts to the recipient.
2. Create and securely store a key revocation certificate for the keypair generated above for possible future use in the event that the private key component is compromised.
3. Create a (preferably dedicated) email address and mailbox to which students may direct transmissions of signed school transcripts.
4. Publish on the world wide web both the dedicated transcript email address and the public component of the OpenPGP keypair generated above, together with its OpenPGP fingerprint.
5. Securely store the private component of the OpenPGP keypair generated above and guard its use with a judiciously chosen passphrase known only to the transcript recipient.
6. Assemble a collection of public OpenPGP keys published by legitimate transcript originators.
7. Receive and decrypt transcripts transmitted by students.
8. Validate the origin and integrity of each received transcript using the public OpenPGP key of the relevant transcript originator.

The similarity between the EESST transcript format and generic OpenPGP / MIME email messages allows transcript recipients to inspect, verify, and extract received school transcripts using existing, widely-deployed email clients. By using email client applications that support both the MIME and OpenPGP standards, transcript recipients should easily be able to verify the signature of the transcript originator and to save the various transcript components locally for later review or processing.

Using familiar email client applications for receiving and reviewing small numbers of received school transcripts does not preclude using more automated systems to meet the needs of university admissions departments or large employers. Larger-volume transcript recipients might ask students to direct their school transcripts to a particular email mailbox. Transcripts so delivered could be periodically received, validated, and otherwise organized by specialized application software. Information in the computational component of received transcripts might be incorporated into a candidate database to simplify more quantitative evaluations of the applicant pool.

4. Transcript Content

The content of a school transcript is represented as a single MIME body part whose content type is `multipart/mixed`. This multipart representation comprises individual MIME elements that represent (in order) prefatory comments from the transcript originator regarding the validation and interpretation of the represented transcript (described in Section 4.1), a rendering of the relevant school transcript suitable for automated processing (described in Section 4.2), and a rendering of that same school transcript suitable for human review and consideration (described in Section 4.3). Figure 3 below schematically presents the MIME structure used to represent transcript content; Figure 4 illustrates an example representation of transcript content.

Every representation of transcript content MUST include exactly the following set of of MIME content headers:

Content-Type:	This header is defined in section 5 of the MIME format specification [19] and, when associated with the content of a signed school transcript, MUST have the value `multipart/mixed`.
Content-Description:	This header is defined in section 8 of the MIME format specification [19]. Its value provides humans with "descriptive information" about the content of the represented school transcript. Notwithstanding the statement in RFC 2045 that a content description header is optional, this header MUST be included in the MIME representation of school transcript content.
MIME-Version:	This header is defined in section 4 of the MIME format specification [19]. Its value identifies the version of the MIME standard to which the associated body part conforms. Currently, the value of this header MUST always be `1.0`. Sometimes, the EESST specification can require an appearance of the MIME version header where it is not otherwise strictly required by the MIME format specification. These seemingly gratuitous MIME Version headers are deliberately introduced to help users who may need to apply less capable email clients recursively in order to navigate and display a transmitted transcript.
Eesst-Version:	The value of this header identifies the version of the EESST format to which the represented school transcript conforms. Currently, the value of this header MUST always be `1.0`.
From:	The value of this header identifies the originator of the represented school transcript. This value names the originating official, his organizational title, and includes, enclosed within angle brackets, the identity of the OpenPGP key with which the represented school transcript has been digitally signed.
Organization:	The value of this header identifies the secondary school that has issued the represented school transcript. By convention, the value of this header names the originating institution along with its geographical location.
Subject:	The value of this header provides humans with "descriptive information" about the semantic content of the represented school transcript. Inclusion of this header is optional, but, if included, its value MUST match that of the `Content-Description` header above. The presence of the `Subject` header helps some email reader applications to present school transcript transmissions more elegantly.

Date: The value of this header identifies the date on which the represented school transcript was created, and its format MUST be consistent with section 3.3 of the Internet standard for email messages [20].

With the exception of the optional `Subject` header, all headers enumerated above must adorn each MIME body part that represents the aggregate content of a school transcript. No other headers are permitted, and the allowed set of headers may appear in any order. Example MIME headers for transcript content are presented in Figure 4.

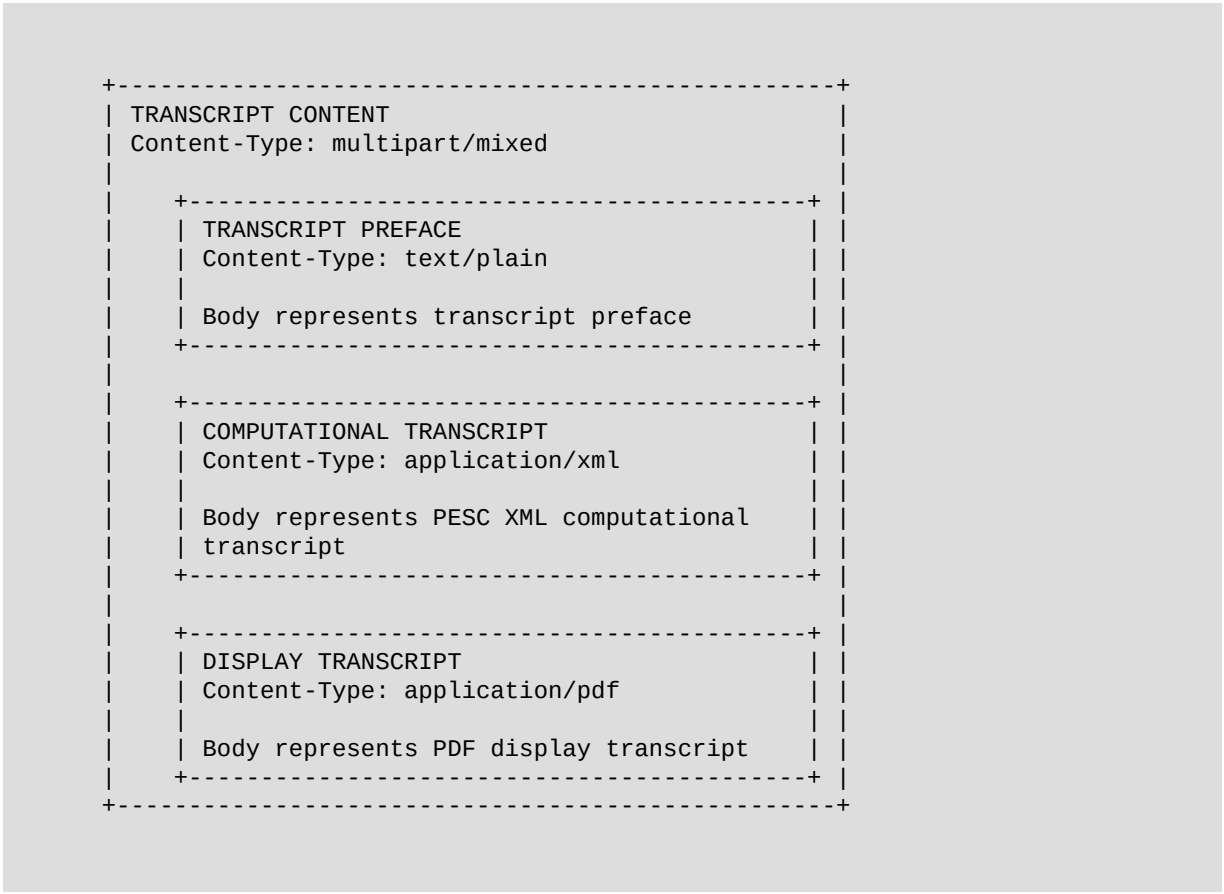

Figure 3: MIME Structure of Transcript Content

```
Content-Type: multipart/mixed; boundary="===============BBBBBBBBBB=="
MIME-Version: 1.0
Content-Description: Official School Transcript for Hermione Granger
Subject: Official School Transcript for Hermione Granger
From: Transcript Authority at Hogwarts School
    <transcript-authority@hogwarts.edu>
Organization: Hogwarts School for Witchcraft and Wizardry
Eesst-Version: 1.0
Date: Fri, 22 Mar 2013 09:55:06 -0600

--===============BBBBBBBBBB==
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment; filename="preface.txt"
Content-Description: School Transcript Preface

To Whom It May Concern:

This academic transcript describes the accomplishments of an
    ...

--===============BBBBBBBBBB==
Content-Type: application/xml
MIME-Version: 1.0
Content-Transfer-Encoding: quoted-printable
Content-Disposition: attachment; filename="transcript.xml"
Content-Description: School Transcript rendered as PESC XML

<HSTrn:HighSchoolTranscript=20xmlns:AcRec=3D"urn:org:pesc:sector:Acad
    ...
cord></Student></HSTrn:HighSchoolTranscript>
--===============BBBBBBBBBB==
Content-Type: application/pdf
MIME-Version: 1.0
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="transcript.pdf"
Content-Description: School Transcript rendered as PDF

JVBERi0xLjMNCiWTjIueIFJlcG9ydExhYiBHZW5lcmF0ZWQgUERGIGRvY3VtZW50IGh0d
    ...
IC9Sb290IDEwIDAgUg0KIC9TaXplIDE2ID4+DQpzdGFydHhyZWYNCjE3OTIzDQolJUVPR

--===============BBBBBBBBBB==
```

Figure 4: Example Transcript Content

4.1 School Transcript Preface

A school transcript preface conveys generic comments about a school transcript from the originating school official. This commentary is in a form that is widely readable by humans without special application tools. This commentary SHOULD be generic in character, providing general information about the preparation and interpretation of transcripts issued by the originating institution; the transcript preface SHOULD NOT provide information about an individual student. The rhetorical form of a transcript preface is sometimes that of a cover

letter addressed to a generic transcript recipient. For example, a preface could provide instructions on how to verify the digital signature on the transcript or an explanation of unusual grading practices at the issuing school. A school transcript preface is represented as a MIME body part whose content type is `text/plain`.

When a school transcript is encapsulated for transmission into a larger email message, arbitrary text within a transcript preface could be accidental misinterpreted as structural MIME boundaries or email headers. The likelihood of such errors is reduced when preface content does not include lines that begin with hyphen (-) characters, angle bracket (>) characters, or the word "From." Although, ideally, the transcript preface should be readable by humans without special assistance, when these constructs absolutely cannot be avoided within preface text, transcript originators SHOULD apply a content transfer encoding to the preface that insulates it from misinterpretation by intermediary mail transfer agents.

The representation of a transcript preface SHOULD NOT include any header fields beyond those enumerated in the specification for the format of MIME message bodies [19].

4.2 Computational School Transcript

A computational school transcript represents the academic accomplishments of an individual student in a form suitable for automated processing. Accordingly, the content of a computational school transcript is rendered in Extensible Markup Language (XML) [7] and conveyed as a MIME body part whose content type is `application/xml`. The syntax of the data conveyed by a computational transcript MUST conform to the XML schema for High School Transcripts, Version 1.3.0 [3], published by the Postsecondary Electronic Standards Council (PESC). This XML schema depends in turn upon the Academic Record XML schema, Version 1.7.0 [5] and the Core Main XML schema, Version 1.2.0 [4], also published by PESC. Detailed semantics for the data elements defined by these XML schema are defined in the PESC XML implementation guide, Version 1.3.0 [2], which also provides usage examples.

In order to protect student privacy, this specification does not require a school transcript to convey any particular student information but, rather, defines only a common format for whatever student information may be voluntarily exchanged between consenting parties. The scope of the information exchanged is a completely local matter, and a transcript originator MAY omit from transcript content any information (e.g., a student's social security number, the identity and location of a student's parents, a student's race, ethnicity, or transgender status) that might be regarded locally as sensitive or irrelevant. Indeed, the requirement that a computational transcript conform syntactically to the PESC XML schema imposes few, if any, constraints upon the transcript originator's choices regarding transcript content. Figure 5 illustrates a minimal set of XML elements that satisfies the syntactic requirements of the PESC XML schema. A computational transcript need convey no more information about an individual student than what little is conveyed by that figure.

In order to prevent implicit monitoring and control of student interactions with transcript recipients, this specification restricts certain uses of the PESC XML schema by transcript originators. In every computational transcript, the `Destination` sub-element of the `DataTransmission` element MUST convey no distinguishable information and have the particular representation

```
<Destination><Organization/></Destination>
```

that is illustrated in Figure 5. This requirement assures that a student may use self-made copies of a signed transcript document for whatever purposes he/she chooses without further consultation with issuing school officials. If the transcript originator is allowed to brand particular destinations onto each copy of a student transcript, then the originator can easily monitor and (to some degree) control the set of college admissions officers, prospective employers, or other third parties to whom the student is providing that transcript. Transcript recipients MUST reject any transcript whose content in any way specifies or restricts the audience, recipient, or distribution for that transcript. Notwithstanding this restriction upon the `Destination` element, the `Source` element SHOULD be included within a computational transcript and convey information sufficient to identify the secondary school or other institution by which the relevant transcript is issued.

```
<HSTrn:HighSchoolTranscript
 xmlns:HSTrn="urn:org:pesc:message:HighSchoolTranscript:v1.3.0"
 xmlns:AcRec="urn:org:pesc:sector:AcademicRecord:v1.7.0"
 xmlns:core="urn:org:pesc:core:CoreMain:v1.12.0"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:org:pesc:message:HighSchoolTranscript:v1.3.0
                     HighSchoolTranscript_v1.3.0.xsd">
  <TransmissionData>
    <DocumentID>X</DocumentID>
    <CreatedDateTime>2011-04-04T09:30:47-05:00</CreatedDateTime>
    <DocumentTypeCode>StudentRequest</DocumentTypeCode>
    <TransmissionType>MutuallyDefined</TransmissionType>
    <Source>
      <Organization/>
    </Source>
    <Destination>
      <Organization/>
    </Destination>
  </TransmissionData>
  <Student>
    <Person>
      <Name/>
    </Person>
    <AcademicRecord/>
  </Student>
</HSTrn:HighSchoolTranscript>
```

Figure 5: A Minimal Set of PESC XML Elements

Additional restrictions on the use of the PESC XML schema foster common, unambiguous interpretation and simplified processing of computational transcripts:

1. In order to satisfy the minimal syntactic requirements of the PESC XML schema, every computational transcript MUST comprise at least those XML elements that appear in Figure 5. Even when a transcript originator seeks to convey no information within a computational transcript, the computational transcript must be included within the relevant transcript content, and its payload must have the form illustrated in Figure 5.
2. Consistent with the PESC XML schema, any value ascribed to the `DocumentID` XML element must be at least one non-whitespace character in length.
3. Consistent with the PESC XML schema, any value ascribed to the `CreatedDateTime` XML element must have the form of an XML `dateTime` value, as defined in section 3.2.7 of the XML Schema Datatype specification [8].
4. Lest the origin and correct handling for a computational transcript be misunderstood, the value ascribed to the `DocumentTypeCode` XML element MUST be `StudentRequest`.
5. Lest the origin and correct handling for a computational transcript be misunderstood, the value ascribed to the `TransmissionType` XML element MUST be `MutuallyDefined`.
6. With the exception of those XML elements that appear in Figure 5, information that is not provided in a computational transcript MUST be represented by entirely omitting the relevant XML data element; omitted information MUST NOT be represented by including an XML element whose textual value is of zero length or contains only whitespace.

The representation of a computational transcript SHOULD NOT include any header fields beyond those enumerated in the specification for the format of MIME message bodies [19]. Although any valid content

transfer encoding is acceptable for a computational school transcript, the `quoted-printable` encoding is preferred.

4.3 Display School Transcript

A display school transcript describes the academic accomplishments of an individual student in a form suitable for human reading and review. A display school transcript is represented as a MIME body part whose content type is `application/pdf` and whose content conforms to the Portable Document Format (PDF) specification [6]. A display school transcript may comprise one or more physical pages.

In order to reduce the chance that the recipient of a signed school transcript could misinterpret its content, the computational component (described in Section 4.2 above) and the display component (defined here) of each signed school transcript SHOULD, to the greatest degree possible, convey identical information about the academic accomplishments of the relevant student.

Nothing in this specification should be construed as requiring implementation or use of digital signature features embedded in individual PDF documents pursuant to the PDF specification. Rather, the data integrity and origin identity of all components in a school transcript --- including the PDF display transcript --- are adequately protected by the OpenPGP signature of the transcript originator, required by this specification. Accordingly, implementation of PDF-specific signature features is optional and largely unwarranted; although transcript recipients MUST accept transcripts that include PDF signatures, recipients SHOULD neither verify nor depend upon the embedded signatures themselves.

Transcript originators MUST NOT use the encryption features described in the PDF specification to encrypt a display school transcript. The OpenPGP encryption mechanisms specified in Section 6 below adequately protect the confidentiality of student information while in transit. Thus, separately encrypting the display transcript is redundant. Double encryption increases implementation complexity while also increasing security risk by requiring additional key distributions. Transcript recipients MUST NOT accept or process school transcripts for which the PDF display component is independently encrypted.

Previous work [18] identifies security considerations arising from using the PDF as a MIME media type. Among these considerations is that PDF documents may include executable "scripts" or references to external, executable plug-in modules. Including arbitrary executable programs (or references thereto) in a PDF transcript document poses a security risk to transcript recipients. Digitally signing PDF documents (or even the transcripts that contain them) does not help transcript recipients to evaluate the safety of executing any embedded programs or plug-ins. The primary purpose of using PDF is to present static transcript information in an attractive format for human review. Because this limited purpose is admirably served without embedding executable elements in PDF files, any risk posed by their inclusion is unwarranted. Accordingly, transcript originators MUST NOT include in a PDF display transcript any executable scripts or external plug-in references; in order to preclude execution of untrusted programs on their local system. transcript recipients SHOULD use only trusted tools to process and view display transcripts,

The representation of a display school transcript SHOULD NOT include any header fields beyond those enumerated in the specification for the format of MIME message bodies [19].

5. Signed School Transcript

A signed school transcript is a MIME body part whose form corresponds to that of a signed OpenPGP / MIME message, as described in section 5 of the OpenPGP / MIME specification [13]. Accordingly, the MIME content type of a signed school transcript is `multipart/signed`, and its form reflects the traditional use of multipart MIME structures to secure email communication [17]. Thus, the body of a signed school transcript comprises exactly two parts, as illustrated in Figure 6. The first part of the signed transcript body conveys the transcript content, in MIME canonical format, including an appropriate set of MIME content headers. The form and interpretation of the transcript content is described in Section 4 above. The second part of the signed transcript body is the school transcript signature. The signature part represents the OpenPGP digital signature of the transcript originator as it has been applied to the transcript content conveyed by the first part of the signed transcript. The transcript signature is assigned the content type `application/pgp-signature`. Transcript recipients MUST reject transcripts that are not validly signed pursuant to the standard for OpenPGP signatures [13].

Figure 6: MIME Structure of Signed Transcript

With the sole exception of the `Content-Type` header, the MIME content headers for each signed school transcript MUST correspond exactly to those for the embedded transcript content, as described above in Section 4. For a signed school transcript, the value of the `Content-Type` header MUST be `mulipart/signed`, its parameters MUST conform to those described in section 5 of the MIME / OpenPGP specification [13], and the value of the `boundary` parameter shall, of course, differ from all other boundary parameter values within the same message. Figure 7 presents example headers for a signed school transcript. Although the allowed headers may appear in any order, transcript recipients MUST reject signed transcripts for which the set of included headers differs from the set of headers associated with the embedded transcript content.

```
Content-Type: multipart/signed;
    protocol="application/pgp-signature";
    micalg="pgp-sha1";
    boundary="===============AAAAAAAAAA=="
MIME-Version: 1.0
Content-Description: Official School Transcript for Hermione Granger
Subject: Official School Transcript for Hermione Granger
From: Transcript Authority at Hogwarts School
    <transcript-authority@hogwarts.edu>
Organization: Hogwarts School for Witchcraft and Wizardry
Eesst-Version: 1.0
Date: Fri, 22 Mar 2013 09:55:06 -0600

--===============AAAAAAAAAA==
Content-Type: multipart/mixed; boundary="===============BBBBBBBBBB=="
MIME-Version: 1.0
Content-Description: Official School Transcript for Hermione Granger
    ...  Transcript Content as illustrated in Figure 4  ...

--===============BBBBBBBBBB==--

--===============AAAAAAAAAA==
Content-Type: application/pgp-signature; name="signature.asc"
MIME-Version: 1.0
Content-Description: OpenPGP signature
Content-Disposition: attachment; filename="signature.asc"

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.10 (GNU/Linux)

iQEcBAABAgAGBQJRmkkLAAoJEBzD54azv/d4j4gH/1Aj8poEHLsEhxdv26H76URX
    ...
8/SQRZGUGUC0xSej5uQMVI59Yriy3dedlzib7EadK6fnz70SsEzUcQy5lHFkNNA=
=8QLW
-----END PGP SIGNATURE-----

--===============AAAAAAAAAA==--
```

Figure 7: Example Signed School Transcript

The `Eesst-Version` header serves a crucial if non-obvious purpose for protocol implementors. The presence of this header unambiguously distinguishes a signed school transcript from elements of an enveloping email message by which that transcript may be conveyed.

For good reason, the format defined here for signed school transcripts intentionally shares many characteristics with the standard format for OpenPGP / MIME messages [13]. This similarity not only admits some code re-use within recipient implementations, but, most importantly, also allows transcript recipients to inspect, verify, and extract received school transcripts using existing, widely-deployed email clients.

However, the formal similarity between signed school transcripts and generic signed messages can complicate recipient implementations of the transcript exchange protocol, because every signed body part must be fully evaluated to determine its status. When a signed school transcript is conveyed to its recipient enclosed within a signed OpenPGP email message, both transcript and conveying message share the common MIME type `multipart/signed`. Moreover, both signed transcript and its conveying message share a common, high-level structure comprising exactly two MIME body parts, independently representing the signed content and the

applied digital signature. When a `multipart/signed` MIME body part is encountered as part of a received email message, should that body part be construed as a proper signed school transcript, a signed email message by which a school transcript is conveyed, ill-formed school transcript, or something else altogether? Without additional information, unambiguously answering these questions requires that every signed body part be fully verified, parsed, validated, and checked, because, absent additional information, a receiving implementation cannot know what tests need to be applied.

Thus, the `Eesst-Version` header serves at least two important functions. Most obviously, this header identifies what version of the EESST format has been applied in preparation of the relevant transcript. Although, currently, the only acceptable version of the EESST format is 1.0, to deny even the possibility of future protocol evolution is to deny the lessons of history. Less obviously, the `Eesst-Version` header allows simple, unambiguous detection of signed school transcripts while still allowing transcript recipients to validate and review school transcripts using familiar, widely-available email clients. For these reasons, the `Eesst-Version` header MUST be included in signed school transcripts and their content component, but, in order to most fully realize its value as syntactic disambiguator, the `Eesst-Version` header MUST NOT appear anywhere else.

6. Transcript Transmission

Provided that the transcript originator is prohibited from disclosing personal information without student consent, use of the EESST protocol empowers each student to limit sharing of his or her own school transcript to recipients chosen by that student. The design of the protocol not only protects the confidentiality of transcript content in transit but also increases the cost of surveillance by the school or other interest parties of the student's interactions with colleges, prospective employers, or other third parties.

A student may convey his signed school transcript to his chosen recipient using any medium or technology that is agreeable to them both. For example, a student may copy his signed digital transcript onto a CD-ROM storage disk and send that physical medium to his intended recipient via a postal mail service. However, because email will frequently be the most convenient means for students to distribute their transcripts, this specification defines a common email format by which each student may privately convey his/her signed school transcript to each recipient. A common form for transcript transmission simplifies implementations of the transcript exchange protocol and fosters their interoperability. A common format allows high-volume transcript recipients to automate decryption and validation of received transcripts as well as their preparation for subsequent review and analysis. A common format that derives from extant email standards allows low-volume transcript recipients to use popular email client software to receive, decrypt, validate, and review transcripts.

When a student conveys his transcript to a recipient via email, that student's confidential transcript information is vulnerable to interception and disclosure. In order to mitigate this threat, this specification generally requires that the conveying email message be encrypted as described in the OpenPGP standard [13]. Every transcript recipient MUST be prepared to accept all transcript transmissions that are encrypted as described in any of the sections below. A student SHOULD use either the Encrypted transmission format (Section 6.1) or the Encrypted and Signed transmission format (Section 6.2), if he or she independently trusts that the transmitting computer will correctly transmit his or her transcript according to the OpenPGP / MIME standard without disclosing its plaintext content. Otherwise, students MAY use the Encrypted File transmission format (Section 6.3) or Traditional Inline transmission format (Section 6.4) below. These latter formats simplify using a more trusted computer to encrypt a student's transcript and later transferring its encrypted form to a less trusted computer for transmission to the chosen recipient.

Because transcript transmissions must be encrypted in order to assure student privacy, every potential transcript recipient MUST generate an OpenPGP key pair and publish its public component for use by students in the preparation of those transmissions. The public key for each transcript recipient should be published (together with its OpenPGP fingerprint) on the web page for that recipient or in the global OpenPGP key database. To protect the privacy of personal information transmitted to each chosen recipient, a student need only retrieve the published key for that recipient and use it to encrypt the transcript transmission.

With some effort, however, an attacker could, by masquerading as a legitimate transcript recipient, perhaps trick a student into transmitting private information to the attacker, encrypted in a key that is known to the attacker. In order to protect student privacy in the face of such attacks, a transcript recipient should resist successful forgery of his/her OpenPGP identity by asking other trustworthy individuals (e.g., respected colleagues or institutional officers) to certify that identity. An OpenPGP identity is certified by affixing another's digital signature to the associated OpenPGP key (see section 12 of the OpenPGP message format specification [16] and section 3 in the GNU Privacy Handbook [9]). Those who sign a recipient's public key are implicitly vouching for the association between that key and the true identify of the recipient. Consistent with the view that the student bears primary responsibility for the privacy of his/her transcript information, the student is ultimately responsible for evaluating the authenticity of public keys that he/she uses to encrypt that information while in transit. Adding certifying signatures to a recipient's key reduces the chance that a student could be deceived by an imposter.

In order to maximize student privacy and autonomy, the operation of this protocol sharply separates the function of transcript creation from the function of transcript transmission. The former function is assigned exclusively to the issuing secondary school (the transcript originator), while the latter function is assigned exclusively to the individual student. Participants in the protocol must behave so as to preserve the privacy

afforded by this separation. A transcript originator MUST NOT transmit, share, or distribute a school transcript or any component thereof to any party other than the individual student to whom it pertains. A transcript recipient MUST reject any transcript that seems to have been transmitted by or on behalf of anyone but the student. Although non-student transcript transmission can be difficult to detect reliably, certain transmission characteristics unambiguously suggest abuse of student prerogatives. Accordingly, all recipient implementations MUST detect and reject transcript transmissions with any of the following characteristics:

- A transcript recipient MUST reject any transcript that is delivered in the same email message or on the same physical storage medium as any other.
- A transcript recipient MUST reject any transcript for which the transcript originator and the sender of the transcript transmission are identical.
- A transcript recipient MUST reject any transcript for which the transcript originator (who signs that transcript) and the signer of the transcript transmission are identical.
- A transcript recipient MUST reject any transcript for which the received transcript transmission is addressed to multiple recipients.

6.1 Encrypted Format

In the encrypted transmission format, the signed school transcript is conveyed to a single recipient as a MIME attachment to an OpenPGP encrypted email message. Consistent with section 4 of the OpenPGP / MIME specification [13], the transmission email message must have MIME content type `multipart/encrypted`, and, as illustrated in Figure 8, the body of the message must comprise exactly two parts. The first body part must have MIME content type `application/pgp-encrypted`, and its content must include only the literal value

```
Version: 1
```

on a line by itself.

The second body part must have MIME content type `application/octet-stream`. Its content is the result of applying the OpenPGP encryption algorithm to the MIME canonical representation of the relevant signed school transcript.

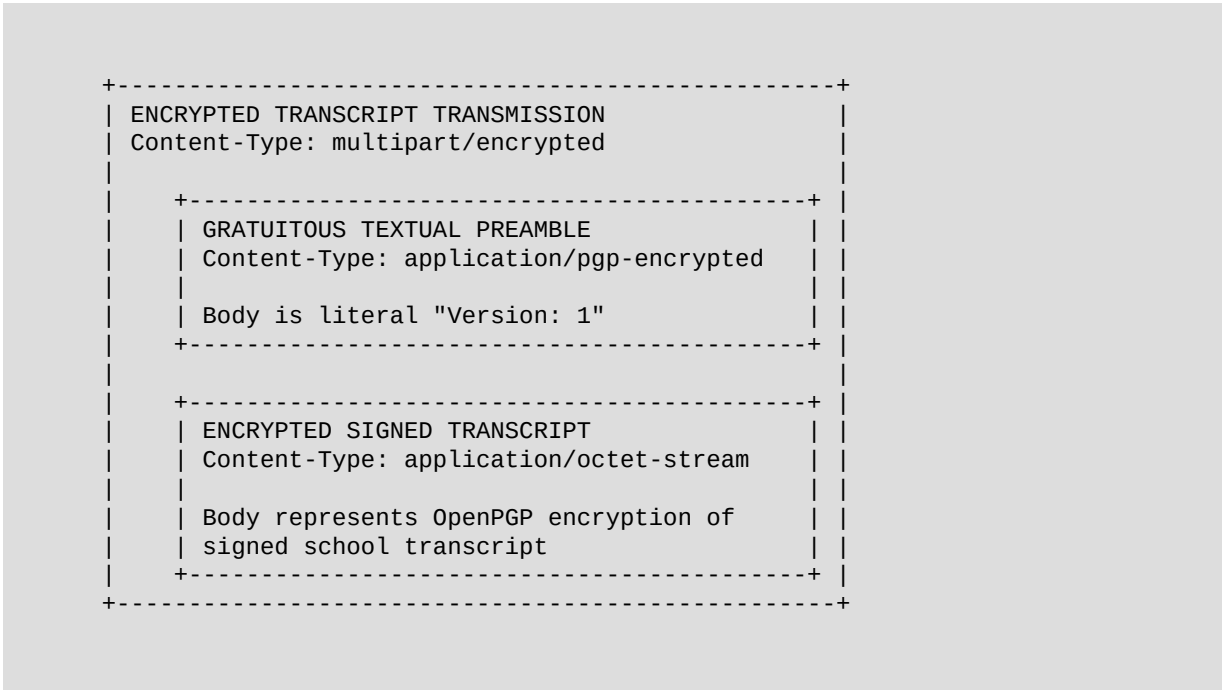

Figure 8: MIME Structure of Encrypted Transcript Transmission

6.2 Encrypted and Signed Format

In the encrypted and signed transmission format, the signed school transcript is conveyed to a single recipient as an attachment to an OpenPGP encrypted and signed email message. Consistent with section 6.1 of the OpenPGP / MIME specification [13], preparation of a message in this format is a two-stage process. During this process, the transcript transmission is, first, digitally signed by the transmitting student and, second, encrypted to protect student information from disclosure to anyone but the lone recipient.

Figure 9: MIME Structure of Signed Transcript Transmission

The first stage of preparing an encrypted and signed transcript transmission applies the student's signature to the transmission content. As illustrated in Figure 9, the resulting MIME body part has content type `multipart/signed` and comprises exactly two parts. The first part is the signed transmission content and corresponds to the signed school transcript in its entirety, whose structure is illustrated in Figure 6. The second part is the transmission signature. Its MIME content type is `application/pgp-signature`, and its content is the result of applying the OpenPGP signature algorithm, using the student's private key, to the transmission content, the canonical representation of the signed school transcript, which is already signed by the transcript originator.

Figure 10: MIME Structure of Encrypted Transcript Transmission

The second stage of preparing an encrypted and signed transcript transmission wraps the result produced during the first stage into an OpenPGP encrypted message, protecting student information from disclosure to anyone but the lone recipient. As illustrated in Figure 10, the encrypted transcript transmission has the form proscribed in section 6.1 of the OpenPGP / MIME specification. The MIME content type is `multipart/encrypted` and the result comprises exactly two body parts. The first body part must have MIME content type `application/pgp-encrypted`, and its content must include only the literal value

```
Version: 1
```

on a line by itself.

The second body part must have MIME content type `application/octet-stream`. Its content is the result of applying the OpenPGP encryption algorithm to the MIME canonical representation of the relevant signed transcript transmission, which was produced during the first stage of the two-stage process.

6.3 Encrypted File Format

Privacy protections afforded by the EESST protocol depend upon the assumption that the computer used by the student to transmit his or her school transcript reliably executes the required EESST protocol operations without disclosing confidential information. In particular, the transmitting computer is assumed to prevent any access to the plaintext form of a school transcript by anyone but the student. The hardware and software of the transmitting computer is assumed to be free of any flaws that could weaken the encryption applied to his or her transcript. The transmitting computer is also assumed to send the transcript reliably and directly to each chosen recipient without reporting to any third party either the fact of this transmission or the identity of the recipient. Validating these assumptions can be especially problematic when the student does not unilaterally own and control the transmitting computer.

Sometimes the computer from which a student must transmit his or her transcript cannot reasonably be trusted. Indeed, some email client implementations manifestly do not permit students to compose a secure email message without sharing private information with either their email provider, system administrator, or other third-party. Web-based email clients are perhaps the most obvious and widespread example of intrinsically insecure email platforms: neither cryptographic keys nor plaintext message content can be safely stored or processed on such systems. Another example of intrinsically insecure platforms are computers and email

servers provided for student use by schools, to which, as a practical matter, school administrators and technical staff enjoy unrestricted access.

A student may use the encrypted file transmission format when the computer that he or she must use to transmit his or her transcript cannot be trusted to perform the necessary encryption correctly or without disclosing the plaintext transcript. This format simplifies using a more trusted computer to encrypt a student's transcript and later transferring its encrypted form to a less trusted computer for transmission to the chosen recipient.

For example, the student may use an implementation of the OpenPGP cryptographic algorithms on a trusted computer to encrypt the plaintext version of his or her signed school transcript, received from the transcript originator. The key used for this encryption is the public OpenPGP key of the intended transcript recipient. The binary file that results from this encryption is then transferred (e.g., via a USB flash drive or networked file transfer protocol) to a less trusted computer for email transmission to the chosen recipient. On this less trusted computer, the student invokes an email client application to compose and send a plaintext email message to the recipient that is formatted according to the Internet standard for Multipurpose Internet Mail Extensions (MIME) [19]. The binary file containing the encrypted version of the student transcript is included in the message as a MIME attachment whose content type is `application/octet-stream`.

When the email message is received by the transcript recipient, the MIME attachment containing the encrypted school transcript may be detached and saved as a binary file on the local disk. A local OpenPGP implementation is invoked to decrypt the saved file using the private OpenPGP encryption key generated by the transcript recipient. The process of detaching and decrypting the attached school transcript may be automated by large-volume transcript recipients.

```
Message-ID: <55650A7F.7090800@granger-dentistry.com>
Date: Tue, 26 May 2015 20:06:23 -0400
From: Hermione Granger <hermione@granger-dentistry.com>
MIME-Version: 1.0
To: Dean Vernon Wormer <transcript-receiver@faber.edu>
Subject: Transmission of School Transcript
Content-Type: multipart/mixed;
 boundary="------------010307000006020005010307"

This is a multi-part message in MIME format.
--------------010307000006020005010307
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: 7bit

Dear Dean Wormer:

Please find attached my high school transcript, encrypted in the
public encryption key published by Faber College for transcript
transmission.  I stored the plaintext signed transcript that I
received from my high school on my own secure computer under the
filename TrnGranger.eml and encrypted its contents for transmission
by invoking the following command:

gpg --encrypt --r transcript-receiver@faber.edu TrnGranger.eml

The resulting encrypted file, TrnGranger.eml.gpg, is attached to
this email message.  Save that file to the disk on your local
computer and decrypt the transcript by invoking the command:

gpg --output TrnGranger.eml --decrypt TrnGranger.eml.gpg

Sincerely,
Hermione Granger

--------------010307000006020005010307
Content-Type: application/octet-stream;
 name="TrnGranger.eml.gpg"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
 filename="TrnGranger.eml.gpg"

hQEMA4Fu2Js7ulkaAQf/aeiLeoy9L+YddGr0HieHd3KH3wiqLnaImsBaLfboGx+EdTIRn
    ...
cSJlVDOZKj6nPULT5zqYsfTEHPf+5escZab4J2Rkt/w1BhNDtulNJrbv6q2lk3xBzlt+Z
kQ==
--------------010307000006020005010307--
```

Figure 11: Encrypted File Transcript Transmission

6.4 Traditional Inline Format

A student may use the traditional inline transmission format when the computer that he or she must use to transmit his or her transcript cannot be trusted to perform the necessary encryption correctly or without disclosing the plaintext transcript. In common with the encrypted file transmission format described above (Section 6.3), the traditional inline format simplifies using a more trusted computer to encrypt a student's transcript and later transferring its encrypted form to a less trusted computer for transmission to the chosen recipient.

The traditional inline format allows a student to use an implementation of the OpenPGP cryptographic algorithms on a trusted computer to encrypt the plaintext version of his or her signed school transcript, received from the transcript originator. The key used for this encryption is the public OpenPGP key of the intended transcript recipient. The encrypted transcript is represented as an ASCII-armored text file that is then transferred (e.g., via a USB flash drive or networked file transfer protocol) to a less trusted computer for email transmission to the chosen recipient. On this less trusted computer, the student invokes an email client application to compose and send a plaintext email message to the recipient. The content of the ASCII-armored file containing the encrypted version of the student transcript is pasted (or otherwise inserted) into the new email message as the sole content of its body.

A traditional inline transcript transmission has the form of a simple email message (in the standard Internet Message Format [20]) whose body is exclusively and entirely the encrypted form of the signed school transcript being transmitted. Representation of the included transcript MUST conform to the OpenPGP Message Format specification [16] for the ASCII Armored encoding of the OpenPGP encryption of the canonical MIME representation of the relevant signed school transcript. An example inline transcript transmission is illustrated in Figure 12.

When the email message is received by the transcript recipient, a local OpenPGP implementation is invoked to extract and decrypt the inline representation of the encrypted school transcript, using the private OpenPGP encryption key generated by the transcript recipient. The process of extracting and decrypting the transmitted school transcript may be automated by large-volume transcript recipients.

While the traditional inline format is an acceptable method of secure transcript transmission, it is probably best suited to students who lack ready alternatives. Because inline representation of OpenPGP messages can sometimes be incompatible with other email features and conventions, the encrypted file format may be a better alternative for transcript transmissions when the transmitting computer cannot be trusted. A brief essay by Josefsson [10] identifies multiple difficulties that can arise from use of inline OpenPGP, although none is strictly relevant to a correctly formed EESST transcript transmission. Accordingly, the traditional inline format may be used when needed but only with full consideration of its potential limitations on interoperability.

```
From hermione@granger-dentistry.com Wed Jul  3 12:41:47 2013
Return-Path: <hermione@granger-dentistry.com>
Delivered-To: transcript-receiver@faber.edu
MIME-Version: 1.0
Content-Disposition: inline
Content-Type: text/plain
Date: Wed, 3 Jul 2013 12:40:01 -0400
From: Hermione Granger <hermione@granger-dentistry.com>
To: Transcript Receiver at Faber College
   <transcript-receiver@faber.edu>
Subject: Encrypted Inline Transmission of School Transcript
X-Mailer: smtp-cli 3.3, see http://smtp-cli.logix.cz
Content-Transfer-Encoding: 8bit
Message-ID: <1372869801.14441.1.camel@hermione>

-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.10 (GNU/Linux)

hQEMA4Fu2Js7ulkaAQf9Fm4+75kE6gQ1T8pjzf4GJhtBqxTTh2AaGtKZkZy9TW8h
zsbSNzZuTVf8QvJRSfk0mZywRG42dilf4Zoygpj3xJgKf7JlCEXnY5m4Luq5hvnW
    ...
hKgY5Kye/cu/4qwYdFOiljkMR1tv1Avh37OmmcMOZ6Hy9gbdrgQzHsPVWLDQNUYy
jxUAN8thZooRj/jHgq23EZaNyKxD
=Dga7
-----END PGP MESSAGE-----
```

Figure 12: Traditional Inline Signed Transcript Transmission

7. Security Considerations

The security of the EESST protocol depends upon the security of the OpenPGP protocols on which it is based. Although the cryptographic algorithms included in OpenPGP are among the strongest used in any known protocol, the integrity, authenticity, and confidentiality of conveyed student information is not assured unless EESST protocol implementors and users faithfully observe all requirements and recommendations of the relevant specifications [16], [13], [15]. In particular, use of the SHA-256 digest algorithm and RSA key lengths of at least 2048 bits are currently recommended and supported by all major OpenPGP implementations.

7.1 Originator Private Key

The authority and integrity of generated school transcripts depend on the continued secrecy of the private cryptographic key by which those transcripts are signed. For greatest security, the guidance director should be physically present when and where the computer program is invoked to generate and sign the transcripts.

When an OpenPGP public-private key pair is generated for use by a transcript originator, a key revocation certificate should also be generated and securely stored. In the event that the generated key pair is compromised, the stored revocation certificate may be used to notify others to reject subsequent uses of that key.

7.2 Originator Public Key

The public cryptographic key for each transcript originator should be published (together with its OpenPGP fingerprint) on the web page for the originating institution and/or in the global OpenPGP key database. Instructions for retrieving and validating the originator's public key should be included in the preface of all issued transcripts.

An association of school guidance professionals may wish to publish an online collection of OpenPGP public keys submitted by their members. A college admissions officer (or other high-volume transcript recipient) could then download and import this key collection into a local key database for use in verifying received transcripts.

7.3 Originator Certification

In order to reduce the chance that an imposter might successfully masquerade as a particular transcript originator and substitute a false key for the authentic one, the identification of each transcript originator with a particular OpenPGP key should be certified by other well-known, trustworthy officials. To this end, the public key for a transcript originator should be signed by other officials of the originating secondary school, e.g., its principal, senior faculty, or local school board members. The OpenPGP public keys of these certifying officials should be published.

7.4 Recipient Public Key

The public cryptographic key for each transcript recipient should be published (together with its OpenPGP fingerprint) on the web page for the receiving institution and/or in the global OpenPGP key database.

7.5 Secure Clients

The cryptographic operations upon which the security properties of this protocol depend must be performed in private by the relevant stakeholder. The confidentiality of a student's personal transcript information cannot be sustained if others enjoy unauthorized access to that content during the process of encryption. The integrity of an originator's signature on each transcript cannot be assured if others can learn the originator's secret key by observing the signature process. The confidentiality of personal information sent by many students to a particular transcript recipient cannot be assured if others can learn that recipient's secret key by observing the decryption of received transcripts. Therefore, every stakeholder should perform the cryptographic operations proscribed here only when present at a physically isolated computer that is entirely controlled by

that stakeholder and that locally stores all keys and confidential information. Using "thin clients" or web-based computing to perform sensitive cryptographic operations forfeits whatever protections this protocol might have otherwise afforded.

7.6 Automatic Replies

Recipient implementations should not reply automatically or routinely to received transcript transmissions. Such replies could provide valuable feedback to an attacker, especially if they can be elicited at will.

8. Acknowledgements

Paul Hoffman and Werner Koch provided independent reviews of this memo. Fred Baker, Dave Crocker, Keith Moore, and Chris Newman provided comments and questions about earlier drafts.

9. References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] Stewart, T., "Implementation Guide for the Postsecondary Electronic Standards Council XML Standard Format for the High School Transcript, Version 1.3.0", July 2012.

[3] Funck, J., "XML Schema for the PESC Format for High School Transcripts, Version 1.3.0", June 2012.

[4] Marton, B., "XML Schema for the PESC Format for Core Main Data Elements, Version 1.2.0", February 2006.

[5] Funck, J., "XML Schema for the PESC Format for Academic Record Data Elements, Version 1.7.0", June 2012.

[6] Adobe Systems, Inc., "Document Management - Portable Document Format - Part 1: PDF 1.7, First Edition", July 2008.

[7] Sperberg-McQueen, C., Maler, E., Paoli, J., Bray, T., Cowan, J., and F. Yergeau, "Extensible Markup Language (XML) 1.1 (Second Edition)", World Wide Web Consortium Recommendation REC-xml11-20060816, August 2006.

[8] Biron, P. and A. Malhotra, "XML Schema Part 2: Datatypes Second Edition", World Wide Web Consortium Recommendation REC-xmlschema-2-20041028, October 2004.

[9] Ashley, J., "The GNU Privacy Handbook", 1999.

[10] Josefsson, J., "Inline OpenPGP Considered Harmful", December 2004.

[11] Saltzer, J., Reed, D., and D. Clark, "End-to-End Arguments in System Design", ACM Transactions on Computer Systems 2(4), November 1984.

[12] Carpenter, B., "Architectural Principles of the Internet", RFC 1958, June 1996.

[13] Elkins, M., Del Torto, D., Levien, R., and T. Roessler, "MIME Security with OpenPGP", RFC 3156, August 2001.

[14] Klensin, J., "Simple Mail Transfer Protocol", RFC 2821, April 2001.

[15] Hoffman, P. and B. Schneier, "Attacks on Cryptographic Hashes in Internet Protocols", RFC 4270, November 2005.

[16] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and R. Thayer, "OpenPGP Message Format", RFC 4880, November 2007.

[17] Galvin, J., Murphy, S., Crocker, S., and N. Freed, "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted", RFC 1847, October 1995.

[18] Taft, E., Pravetz, J., Zilles, S., and L. Masinter, "The application/pdf Media Type", RFC 3778, May 2004.

[19] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.

[20] Resnick, P., "Internet Message Format", RFC 2822, April 2001.

Author's Address

James R. Davin
EMail: info@EESST.org
URI: http://EESST.org/