



Receiving Digital Documents

Transcript Research

October 2020



Receiving Digital Documents

In this digital age, how do we know what documents we can accept and from whom?

At Transcript Research, we have long been fans of receiving digital records. This year's school closures, distance learning, online education, and other upheavals have made it even more critical for us to ensure that we are accepting official academic records from valid sources. Sounds enough enough, right? Well... there are caveats and questions.

- Who has sent you the document?
- Using what method?
- Is this in a response to a request that you made to the institution (replying to your email or using a form you provided to the institution), or is this something requested by the student?
- Have you confirmed that they are from the appropriate institution?
- How did you confirm that?
- Is the person who sent the documents to you authorized to send official academic credentials?
- Does the institution's website indicate what department or division of the institution they are from?
- Does the institution even have a working website?
- If the documents were sent by email, were they from an email address that is already listed on the institution's website or government websites, or is it a totally different website?
- Is the email from a gmail, hotmail, yahoo, or other email provider rather than an email address from an institution-specific domain? Is that common? Should we trust it?
- If it is an institution-specific domain email address, how do you know this is from an employee and not from a fellow student at the institution?
- If it is an employee of the institution, have you confirmed that they are authorized to issue or share official academic records?

There are likely more questions than this, but hopefully we will cover the highlights in this document. At our institution, we allow students to provide unofficial copies of their academic records to begin the process, but we require official documents before we are able to finalize and issue our evaluation reports. The definition of official document varies by country and level of study, so we have a pretty detailed list of country requirements on our website. (We also try to send everything for verification, but that is a different story for a different day.) The student needs to make arrangements to send their official documents to us, and we accept digital records as long as we can answer those questions.

To clarify, we do not consider documents sent by the student to be official unless we can verify them. Most of the time, we rely on the official documents to be sent to us. In this article, we are just talking about digital documents so let us limit our focus to that.

Typically, when we are receiving official documents digitally, it starts with an email. This email might be an email telling us we can access a national database, it might be a link from a third-party digital repository, it might be an email from the student telling us where we can download their official digital record directly from the institution's transcript website, or it might be an email from someone at the institution. Let us discuss each of these scenarios so we can explore some of the other questions and



even some of the answers that will help you make good decisions that balance the need to accommodate your students with the need to receive authentic academic credentials.

National Databases

My offices uses a number of electronic tools for verifying educational records. We look for individual contacts at higher education institutions and examination boards. We seek out newspaper lists of graduates. We look in our country resources from conference handouts, industry publications, and international education newsletters to see if we can find mention of verification tools. But we start by looking to see if that country has a national database, and we begin that process by seeking out the Ministry of Education's website to see if they handle national leaving examinations directly, or if that is done by a department or division affiliation to the Ministry.

This is especially true for secondary leaving exams, which have a pretty high propensity of having online databases where third parties can check student results. This also includes some national post-secondary databases that may only allow you to verify information that would be on a graduation document, such as the name of the degree, graduation date, degree program, and possibly the grade point average.

Essentially, we research to see if the national examination authority or Ministry of (Higher) Education maintains a publicly available list of graduates, exam results, or anything else that will allow us greater confidence in a student's records.

At the secondary education level, more than half of the world has some kind of national or state-wide leaving examination that is required of secondary school leavers. A leaving examination allows students to be compared against standardized results for purposes of further education, but it also often leads to standardized documents issued by a centralized body. Due to this standardization, it is increasingly common for us to find that examination bodies or Ministries of Education maintain some kind of electronic database.

Sometimes these databases are very basic and merely contain a list of the students who passed the most recent examination period, such as the French Ministry of National Education, Youth, and Sports, which allows you to examine a list of graduates by *academie* and secondary or technical examinations ranging from the *Diplome National du Brevet* to the *Baccalaureate General* to the *Brevet de Technicien Superieur*.

Sometimes the websites maintain a little bit more information; graduation lists for the past several years may be downloaded or looked up. Such was the case with the official portal for the government Republic of the Guinea or the website for the Ministry of National Education of Mali. You may have to dig around for the information, because the different data sets are often uploaded to separate web-pages that do not always have a common landing page to unite them. That is when your [google site search](#) skills come in handy. Sometimes the websites make it easy to find results or graduation lists as long as you use the local terminology, and other times it takes more digging.

There are also instances where we hope to find older lists from the national examination board or ministry. While we always try to download the graduation lists to our internal country resources to have



them when needed, sometimes we just do not have any evaluations for that country for that year. But if we have the lists from two years ago, and the website shows the current year's list, it stands to reason that there was a graduation list for last year. That is when we break out our skills with the [Internet Archive](#), also known as the Wayback Machine. While java-based web pages and embedded images do not usually get saved by the Internet Archive, we have had pretty good success with locating older PDFs that have been archived online. We also frequently come across spreadsheets and HTML web pages that hold critical lists of graduates or examination results.

While these examples have all been about secondary level education, we also find that a number of countries maintain national databases of higher education graduates. The United Kingdom's Higher Education Degree Datacheck (HEDD) and Canada's AuraData are examples of some of the paid registries while Kyrgyzstan's State Registration Service, Mexico's National Registry of Professionals, Argentina's Public Registry of University Graduates, and Ukraine's Unified State Electronic Database on Education are just some of the post-secondary national databases that maintain varying levels of information about degrees awarded.

So far, we have only talked about the bare-bones types of information that helps you validate a student has passed a national leaving examination or earned a degree. These systems are important tools to help up with our credential evaluation work, but verification of limited data is not the goal of this article. We specifically want to identify digital tools that allow us to receive an entire student record via a digital source.

While there are many universities around the world that maintain their own digital records that they can share with you, as we shall discuss later, there are not as many opportunities to easily obtain digital records directly from the source without getting the student's express permission. In fact, it is increasingly common for privacy laws to prohibit institutions from sharing digital records until or unless the student requests it. Generally speaking, when this is an option, you must have the student arrange for the national database to send the documents to you electronically. We see this increasingly from the various National Academic Depository providers in India.

Third-Party Digital Repository

Sometimes we hear about digital repositories or secure online transcript platforms like Digitary or Parchment from conferences, industry news, or from our network of credentials evaluators. Sometimes a student tells us about them, and we go digging to find more information. My eEquals is another great tool for records issued by institutions in Australia and New Zealand.

We do not have a hard and fast rule for what third-party digital services we deem acceptable because it depends on a number of factors. We look to see if they have relationships with the government or Ministry of Education in the country or countries where they are based. (Please not that, throughout this document, "Ministry of Education" is used generically to refer to the higher education authorities in each country, even though the name may dramatically differ in that country.) We examine their publicly identified relationships with higher education institutions in the country. We look through conference handouts and on message boards to see if others have asked or explained about them. We peruse their "About Us" information on their website and attempt to confirm information that sounds promising.



Ultimately, our goal is to see if others in the country or region are accepting these documents, who they are, why they feel comfortable, and how long the institution has been doing this work in the country.

In some cases, like the China Academic Degrees and Graduate Education Development Center (CDGDC) and China Higher Education Student Information and Career Center (CHESICC) in China, the organizations are authorized by the Ministry of Education. Parchment (which now includes Credential Solutions and eScrip-Safe) and the National Student Clearinghouse are two established digital credentials services based in the United States that have processed literally millions of transcripts. Digitary has been around for fifteen years and is used by organizations in over 100 countries. Not coincidentally, most of those third-party digital repository providers are signatories of the [Groningen Declaration](#) on digital student data portability.

Generally speaking, if we find that a transcript exchange service is operating, we try to find more information about it. Who runs it? Is it run by the government like Singapore's OpenCerts system or the UK's Higher Education Degree Datacheck, or is it an official service of the educational sector, like the Diploma Registry in Norway or the South African Qualifications Authority? What if it is unclear who owns or operates it, but it has records for all public and private educational institutions, like Canada's AuraData? Is it a privately owned third-party provider like GradIntel in the United Kingdom, eTitulo in Spain, or TrueCopy in India? What about private companies that have relationships with institutions around the world like BC Diploma, who generates block chain certificates for institutions in Canada, France, Tunisia, Senegal, Vietnam, and more? On the flip side, what if they claim a relationship with the higher educational authorities that is later determined to be false; would we still trust documents they provide?

Now that we are getting more questions than answers, you can see why it is hard to have a definitive hard-and-fast rule. We all need a starting point, though, so we check with our network. We look to see if they have a relationship (direct or indirect) with the government or higher education authorities. We look to see how long they have been around. Are they mentioned in our saved conference and presentation handouts or mentioned in industry articles? Have other people asked about them on message boards, mailing lists, social media outlets, or other forums for asking our network? We look to these resources first, but if we do not have any success or are not confident in the outcomes, we reach out to our individual networks of colleagues, country experts, and educational authorities. We ask EducationUSA advisors. We email conference presenters or publication authors. We access ENIC-NARIC Networks. We contact the embassy or the Ministry of Education. And we also post questions ourselves to the various message boards and mailing lists. For single country platforms, we look to see whether universities in that country mention the platform on their own

But what about newer platforms? How do you know when you can trust a new digital provider? All of the private providers we have mentioned above have years, if not decades, of experience behind them, and those years of business are part of why we feel comfortable in their legitimacy. But everybody is new at first, so how do we know if it is safe to trust new providers?

As with so much in our industry, there is not one single answer that encompasses all. It is nuanced and layered and all the other vague ephemeral language that dances around saying, "I don't know." Part of it is reputation, part of it is relationships and connections, part is history, part is legitimacy, and part is probably something I have not even thought about yet. Assuming that we are talking about a private, for-profit organization (since public organizations would likely be authorized by the government



authorities also in charge of the educational system), we look to see who their clients are. Are those universities referencing them on their own websites, both for sending and receiving transcripts? If so, is it an aside or minor notation, or is it prominent, easy-to-find declaration? Does this provider have technical documentation about their security measures to keep payment information and academic records storage and transcripts secure? Is it clear where the platform is getting the academic records? Are they loaded directly from the higher education institution, sent by the institution (digitally or by mail) to the platform, or are they provided by the student and then verified by the platform? Does your acceptance of the platform depend on the answer to that last question?

There are some digital platforms that we are simply not comfortable accepting for a variety of reasons, but we might not have a distinct reason for our discomfort. Perhaps they charge significantly more for digital transcripts than the institutions themselves charge; they claim approval or partnerships with the educational authorities that prove to be false; the internet abounds with complaints about how much longer they take than going in person and ordering original transcripts; they advertise services for all higher education institutions in their country but then only have relationships with a small number; or they threaten legal action against you for simply stating your inability to accept their documents in lieu of your standard document processes for that country. On the other hand, maybe they charge more because they are new in the field and do not have the advantage of the economics of scale that larger or more established companies have. It is possible that they are innovators of a new technology or service in their country and having a slower or harder time getting buy-in from prospective institutions. Maybe they did get an informal approval from higher education authorities that simply is not on those government websites because it is not as important to them as it is to the digital platform. If the HEI is responsible for releasing transcripts to the platform, perhaps delays are legitimately out of the third party provider's control.

Ultimately, we all have to make a decision for our own institutions on which of the transcript exchange platforms we are willing to accept. Luckily, whatever decision you make does not have to be formal and binding. You could tentatively accept a few documents from a new-to-you digital platform and then verify them directly with the issuing institution. Yes, it is more work and time, but if it helps you build confidence in that new platform, it seems worthwhile if that platform has the option to save you and your students time down the road while it increases your confidence in the authenticity of the documents. And if you find you still are not comfortable after your test scenarios, you can always revert to your previous requirements. In the interim, you can let your prospective students know that you accept some digital repositories on an individual review basis. This alerts your students to the fact that you are making accommodations for digital documents without putting you on the spot for specific tools that might not fit your comfort levels.

Institution's Website

Sometimes, we find out from students – or the documents themselves – that we can download the student's entire record from the institution's website. I am not talking about logging in to the internal student registration system as the student to print an unofficial transcript. We do not consider student registration systems to be official records, and they frequently even include language saying that. As an example, Qassim University's Academic Registration site specifically has red text stating that the academic record is not used for official purposes, though other student registration sites are not as clear. The Islamic Azad University's Science and Research Branch online WorkBook (student portal) allows



students to view their unofficial transcripts by semester as tables on the screen. These are just two of many examples of unofficial student records systems that are designed to allow students to see their grades and registration information but are not intended for use by others.

A major reason we do not accept these student registration web pages is because they are not meant to be official and might not even represent final information. Documents or screen-captures from a student registration website would not be considered official at the same institution. In addition, it is common for important elements that would normally appear on the official documents – including graduation date, major, final grade point average, class ranking – to not appear on the unofficial grade sheets on the student portal.

Another, equally important for not using these types of sites is because we would be logging in as the student. Some of these sites strictly prohibit students from sharing their username and password with anyone else (other than an approved parent or caregiver). This might even be a violation of privacy regulations in that country. Many student records systems also include a great deal more information about the student beyond just their unofficial grades; these systems may include personal information, financial or financial aid information, student employment, emergency contacts, upcoming or current registration, current schedule, and so much more. We do not want the liability of logging in to a system that was meant for only the student to access in case something were to happen to their account. We also do not want to be concerned about the privacy implications of logging in as someone else. We use only those institutional websites that are designed for a third party to access in order to download or verify a complete educational record instead. So when I talk about institutional websites, I am not referencing student registration systems or customer relationship management portals.

I am also not referring to semester results checkers that allow you to confirm a student's individual semester examination results. This section also does not include those websites that maintain lists of everyone who graduated, either by academic faculty or by convocation year. It also does not include websites that allow you to enter the student's name, roll number, diploma number, or some other information tied to the student that allows you to confirm graduation. While these are various tools that we use in our evaluation work, they are less inclusive than the kinds of websites I mean.

I am referring instead to institutions that allow you to digitally download the official student's academic record. Sometimes this requires you entering a digital code from the document into the university's portal, which we see from some universities in Italy like the *Universita di Bologna*. This also includes the University College Dublin, which has a neat feature that allows you to enter the student number and document number on a verify portal in order to download the entire transcript. A handful of institutions in India, for example, provide online verification for the entire student record, which allows you to download the full digital record using a bar code number or code. This includes institutions such as the ICFAI Foundation for Higher Education. Contrast this with the much larger number of Indian higher education institutions that only provide online access to the most recent term's examination results.

In other situations, the educational authority may provide you with a link from their website to a direct download of the official student record, such as with the British Columbia Ministry of Education. Sometimes, institutions move away from using a third party product and begin offering their own digital student records, as we see from some universities in South Africa.



We see a similar scenario with some universities. The student logs in to their student portal and can request to have an official digital transcript sent securely to a third party, but it is the university that sends an email to the third party. The email received from the university directs you to a download link that allows you to obtain the full and complete official academic record online.

The same is true for the London School of Economics, with the variation that after you receive the link and login, you have to create an account so they know who is verifying records. The benefit of this for you is that you may be able to re-verify documents at a later date by using the login information and the document reference number if the system allows continued access.

Sometimes, institutions add another layer of security beyond requiring passwords sent by an email generated by a student's request to the institution. You log in to a specific website, enter the password, and then you are able to view the official documents. The caveat is that these documents are marked as Valid Only for Online Viewing. We have seen that at the University of Manchester and other institutions. In those situations, you are expected to be verifying documents already in your possession, but they do not easily allow you to download the academic transcript.

Please be aware that some online portals – both institutional and third-party – only grant you access for a limited amount of time or a limited amount of times to access the results or records. As a result, it is usually a good idea to double-check that you properly saved the official digital document before you move on to your next task.

Another type of institution's website is the examination board. The majority of countries around the world offer a standardized examination at the culmination of upper secondary school. This is frequently referred to as a national leaving examination, though they may instead offer a matriculation examination. Higher education admissions is simplified in these countries because all students preparing for further education are sitting the same examinations that are being graded against the same standards with less subjective grading and emphasis on class ranking. Another benefit of national leaving examinations is that students are issued standardized documents, making it is easier to compare them against sample credentials in your database. These standardized documents issued at a national or statewide level by the same authority have an increased chance of being issued on security paper or having other built-in security features. More importantly for this context, the results of standardized exams have a great chance of being loaded into an online database. Countries with standardized leaving exams are more likely to have online portals to verify or download graduation examinations results.

Look to the West African Examinations Council. WAEC ushered in a new era when they created their revolutionary scratch card system. Their results checker allows anyone in the world (who has the scratch card and a copy of the student's examination certificate) to log in and access the complete examination record with all subjects and grades obtained for that sitting, even results that do not appear on the final certificate. Other examination boards offer similar services where you can enter basic information about a student and verify their entire examination record. The Intermediate and Secondary Education Boards of Bangladesh has a fantastic website that allows you to access the complete secondary and higher secondary examinations data since 1996.

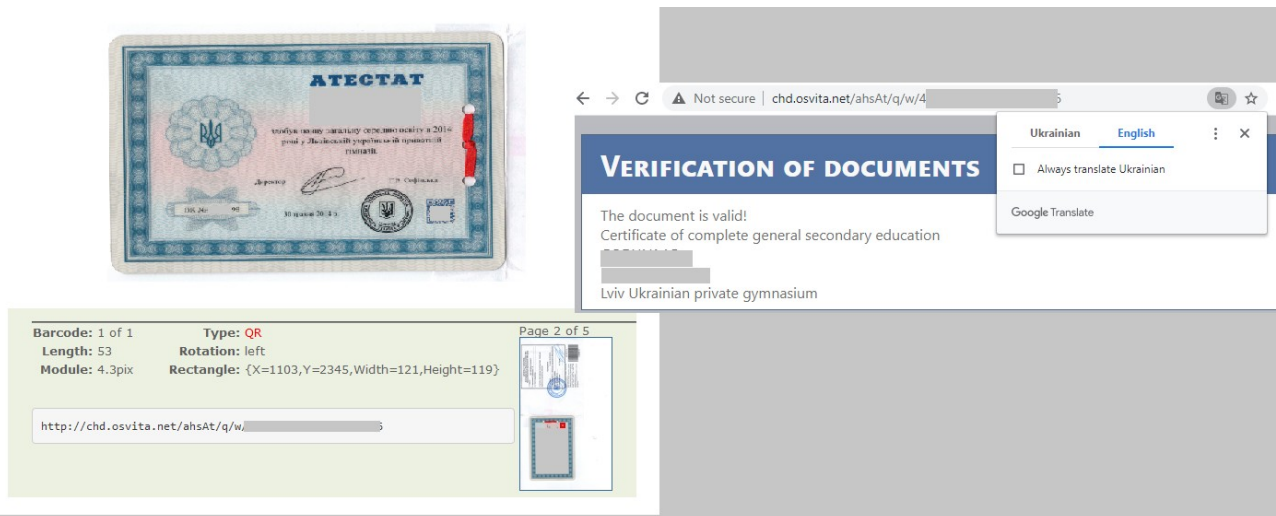
Let us spend a moment talking about QR, or quick response, codes. When we see a QR code on a document, we have mixed reactions. Sometimes, the QR code only works in a QR code reader approved by the institution. We have seen that from WAEC Ghana and WAEC Sierra Leone, CDGDC



(through WeChat), and DigiLocker in India. Generally speaking, though, you can only use those apps from within the country so they do not offer us much help from another country.

On the other hand, we like it when we get QR codes that take us directly to a web page such as the QR code printed on Bilkent University transcripts. When using a QR code app on a handheld device, it shows the URL as a direct link. In this case, it also happens to be printed on the bottom of the transcript: “transcript may be verified at: <https://trn.bilkent.edu.tr/4UUS-38IT-redacted>” This also works for secondary level educational records issued by the the Ministry of Education in Chile and the Ministry of Education in the Dominican Republic. We have also been seeing them as an option for verifying degrees or degree registration in places such as Peru, Ukraine, and Chile. The QR codes from these institutions resolve into a web page where you could have just as easily typed and entered the student’s relevant information to verify these diplomas or graduation examinations. In fact, we highly recommend that you manually navigate to that web page and enter the student’s information there to make sure the website matches what it seems. We use an online QR Code reader to make it easier to both see the URL (and copy and paste it into a separate browser to ensure we can recreate the process) and to save the QR verification output.

The example below is from a QR code from a Ukrainian high school diploma. The upper left image is the diploma, the bottom left is a screen capture from the online QR code reader, showing the URL, which was then copied into the browser on the right.



Sometimes we get a QR code that does not lead anywhere or was not intended to be read by a generic QR code reader, only that institution’s specific QR code app. In those cases, we try to download that institution’s app but have had very little success with that effort, either because the app is not available in our app store since we are in a different country, or because a country-specific phone number is required for registration such as the DigiLocker app. As a result, we are unable to accept those QR codes as proof. We also sometimes get QR codes that are on translated documents, but while the QR code resolves to a website, it is the website of the translation company or government translation body, or the QR code is specific to the apostille rather than the issuing institution.



Note that sometimes you might try to access an institution's website, and it appears the web page is still a valid URL, but it does not appear to be working. If that happens, try using the web page a different browser, or try it in incognito or private mode to eliminate possible interference from browser add-ons. The Certpia website from Korea is one that works better in Firefox than Chrome, for example. It is also a good idea to use the internet to find out what time it is in that country; it is common for institutions to update their databases in the evenings in their local time zone so you might simply be catching them when they are updating or backing up their data.

Email Attachments

And now we come to the trickiest but also most prevalent of the digital records options that many of us are seeing: email attachments. The bulk of this publication will focus on email attachments and security of email and attachments since those seem to be the two most complex aspects of the issue of accepting digital documents.

There are so many things I want to talk about with respect to accepting digital records by email: email headers, types of emails, types of attachments, and security features.

Email Headers

Full email headers are the first thing we need to look at when considering whether or not to accept an email that is not a reply to a request we sent. The reason I include that caveat is because my institution sends out tons of emails to try to verify documents, using our personalized verification form and an internal ID number (not known to the student). When we send our verification request emails, we independently search for the email contacts on the institution's website or social email, our in-house wiki, the TAICEP Verification Sources (which I help maintain), or other resources. When we send those emails, we include our verification form, the student's verification signature release (which we incorporate into our application since verification is so important to us), and the documents, along with the secret internal ID number that is unknown to the student so that we know that the verification email we get is actually in reply to the request that we sent independently to the institution.

I have included links below for how to look up the full email headers through some of the most popular North American email providers:

Gmail: this URL will show you how to look at an email's full headers in Gmail, Hotmail, Outlook,

AOL, and other web-based email services: <https://support.google.com/mail/answer/29436?hl=en>

Microsoft Outlook: <https://support.microsoft.com/en-us/office/view-internet-message-headers-in-outlook-cd039382-dc6e-4264-ac74-c048563d212c>

Proton Mail: <https://protonmail.com/support/knowledge-base/check-email-headers/>

Yahoo! Mail: <https://help.yahoo.com/kb/SLN3276.html?redirect=true>

Mail.com: <https://support.mail.com/email/receiving-and-reading/header.html>

iCloud: <https://support.apple.com/guide/icloud/view-long-headers-mmcc887ce9/icloud>

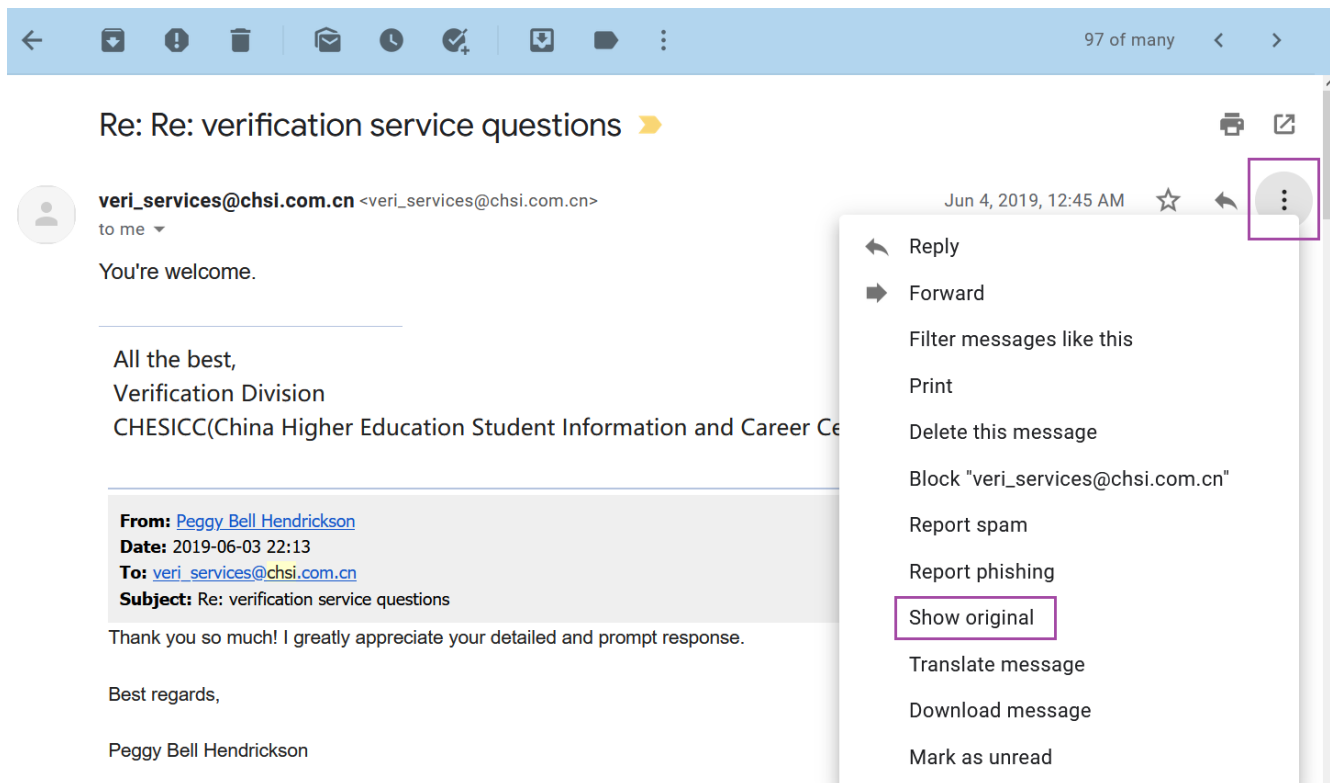
Zoho Mail: https://help.zoho.com/portal/en/kb/campaigns/deliverability-guide/how-to-s/articles/understanding-message-headers#Zoho_Mail

Because my own familiarity is with Google's Gmail, I am going to walk through the steps of looking up the full headers.



First up, you open the email and click on the 3 little buttons that are currently in the upper right hand corner. (Google has a tendency to move things around, so if you read this six months after I have released this article into the wild, it is possible that might not be the case anymore.)

Clicking on the 3 buttons will bring up a context menu. From this menu, you will need to click the option for “Show Original.”



This will open up your email in a separate tab, but now you will have a more thorough version of the email. Like postal mail, an email, or electronic mail, consists of several parts: headers, body, and the envelope. The header is kind of like the mailing information for a postal letter; it has the sender's and receiver's name and mailing information, which you see immediately. If you dig a little deeper, though, you can see the entire route as well as the subject, date, and routing directions. In postal mail, that information is encoded in the bar code and tracking information; in an electronic mail message, that information is in the full email headers. The body contains the text of the email itself. This text might be in plain text or hypertext (HTML) with formatting and links, depending on what the recipient's email displays. The envelope has the actual routing information communicated between the email client (the program you use to send and receive email) and the server that does the work of sending and receiving your messages. The envelope is what actually determines where the email is sent, even if that differs from what is in the headers, just like a postal letter would deliver a letter to the address on the outside of the envelope, even if the letter inside was addressed somewhere else.



By opening up the detailed headers, we can see if the information that is shown on the email matches up to what we think it should be.

Not only will you have full email itself (though hidden in a bunch of HTML), you will also be able to see the detailed header. The next image shows a screenshot of the full headers for the email above.

Original Message

Message ID	<5cf6055f.1c69fb81.2632b.b12cSMTPIN_ADDED_BROKEN@mx.google.com>
Created at:	Tue, Jun 4, 2019 at 12:44 AM (Delivered after 9 seconds)
From:	"veri_services@chsi.com.cn" <veri_services@chsi.com.cn> Using Foxmail 7, 2, 8, 379[cn]
To:	Peggy Bell Hendrickson <peggy@transcriptresearch.com>
Subject:	Re: Re: verification service questions
SPF:	PASS with IP 184.105.206.83 Learn more

[Download Original](#)

[Copy to clipboard](#)

```
Delivered-To: peggy@transcriptresearch.com
Received: by 2002:a17:90a:ff06:0:0:0:0 with SMTP id ce6csp2437441pjb;
Mon, 3 Jun 2019 22:45:03 -0700 (PDT)
X-Google-Smtp-Source: APXvYqxlyxHyYdjMh25n154QaPnYeOPjHEYWAjHp3UqvkvjxN3Vf80pKmqg+Tcv0oT500aZ2dv7+
X-Received: by 2002:ae9:e015:: with SMTP id m2lmr6276200qkk.116.1559627103603;
Mon, 03 Jun 2019 22:45:03 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1559627103; cv=none;
d=google.com; s=arc-20160816;
b=nLlVw40t/brMXFKqxjk737bb0a/HFpLrdcZgyX470V4jEIrxcPW/ess2vYeV/xXc8
13NhsZaio0o0Xn5PVPJlr+aAau0Xa9lwoY2orWcEEmXmk8jwx3WkEMog9Z0RG6333oLN
i6Kp1lz1kc3L8CDrxmL058iyGa9Hks7u8L/p1G9X1f7/HrAV11B3gKZ/8LzQQIqjxI12
dnjL+lyG+QcxTYyt13fXnOGGDJ0HEPukMM/jO/ah8OrY/dbnSDK4F8uViH8EUeRZnsb
yJfp+VLWjQTK9Dsx/IB1N31W2pejDPBbsXJr/hzUhcBnOIq+twJEIgi9REVTLnZ+Ljqs
sVrQ==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
h=feedback-id:mime-version:references:subject:to:from:date:message-id;
bh=VhSHb6a/9VJxLH54y7ef8wloellUY/FVk/izwmaHlQQ=;
b=0TXd0iww2T/INLJr047DM4Y90o5EqOingcdHln80Zsc9MfhbsNqy11U4UxIYrQJddw
9ZccoWorUQZRC/Lp9Lf6Kq054k2qWQuD6nbb5gd9wU0+JzLkRtIEr8yCe7zFIq1Pq1W7
M7nn6jFzPt5WjtS8Fg/UXHd270eykbKx7X0Ie0hxdKGGmHY867Iu+AB/Tg5wXjKPaXh5
o3f7ShdVhEXlINpyvOZTTml5vvpLywdCF13XbFAjSIwXGNDcLt11CmbrWfXeS8zFhCDN
```

Okay, so now you know how to find the headers. But what does that mean, exactly? What are you supposed to do with this overload of information that looks kind of like a cat walked across a keyboard? There are several things you can do. If you think you have been sent a phishing email (where someone pretends to be an institution or person they are not in order to trick you into logging in with your real username and password to a fake website that looks like the real thing so they can steal your information or money), your financial institution will often ask you to forward the email with full headers. The same is true if you get an unexpected email that seems to be from someone you know but has an attachment that you are unsure about. It is very common for people's email accounts to be compromised and for those hacked accounts to spam everyone in the account holder's contacts list with an attached virus since people are more likely to download an attachment from someone they know.



This can be a little overwhelming so let us take a deeper look at the email headers. If yours is a Gmail account, you can use the Copy to Clipboard button to copy the expanded headers into the Google Admin Toolbox Messageheader at <https://toolbox.googleapps.com/apps/messageheader/> so that it can do the heavy lifting to analyze the header.

Google Admin Toolbox Messageheader

Messageid	5cf6055f.1c69fb81.2632b.b12cSMTPIN_ADDED_BROKEN@mx.google.com
Created at:	6/4/2019, 12:44:54 AM CDT (Delivered after 9 sec)
From:	"veri_services@chsi.com.cn" <veri_services@chsi.com.cn> Using Foxmail 7, 2, 8, 379[cn]
To:	Peggy Bell Hendrickson <peggy@transcriptresearch.com>
Subject:	Re: Re: verification service questions
SPF:	pass

#	Delay	From *		To *	Protocol	Time received
0	1 sec	unknown	→	esmt10.qq.com	SMTP	6/4/2019, 12:44:55 AM CDT
1	8 sec	smtpproxy21.qq.com.	→	[Google] mx.google.com	ESMTPS	6/4/2019, 12:45:03 AM CDT
2			→	[Google] 2002:ae9:e015::	SMTP	6/4/2019, 12:45:03 AM CDT
3			→	[Google] 2002:a17:90a:ff06:0:0:0:0	SMTP	6/4/2019, 12:45:03 AM CDT

The Admin Toolbox Messageheader basically lets you know at a glance how likely it is that the email passes certain security features we will be discussing shortly. All of this same information is in the detailed headers, but this tool removes the extraneous information, enters the critical parts into an easy-to-read table, and color codes it as well. When you first begin working with email headers, tools like this can increase your confidence because they pinpoint all the highlights.

This is a pretty neat feature that allows you to see if an email is authenticated, meaning that Google believes that the message is coming from the person who appears to be sending it to you; it is unlikely to be a spoofed email. Email spoofing means that the sender forged the “from” information. This is common for spam emails and phishing emails to try to trick you into believing the email has been sent from a more trustworthy source. Even though we are not dealing with financial information when



talking about receiving a student's digital records, email spoofing is still a big deal. A prospective student may arrange to have a forged email sent to you in order to make it seem like the educational institution is sending their official electronic records to you.

One of the ways you can confirm this is by looking at the first box on the detailed headers to see if there is any information about SPF, DKIM, or DMARC. These are tools identified as the cornerstone of email authentication. SPF, or Sender Policy Framework, is a way for recipients' email providers to confirm the identity of the sender of an incoming email at the domain level. It is one of the fastest ways to identify if a message is being sent from the domain it says it is being sent from, which can land some emails in your junk folder but also might result in an email being rejected altogether. DKIM, short for DomainKeys Identified Mail is a more advanced version because instead of using a single DNS record based on the from: address, it utilizes two encryption keys, public and private. DKIM adds a digital signature to every email that lets the receiving server verify that the email was not forged or modified. DMARC is Domain-based Message Authentication, Reporting, and Conformance, which enforces SPF and DKIM authentication and provides reports to administrations about message authentication. DMARC must be utilized in conjunction with one of the other two because it builds on their technologies about authentication but goes a step further by giving instructions on what to do if the authentication fails. This paragraph is obviously a very non-technical and high level overview of these types of authentication. If you want more information for yourself or your institution, I highly recommend you check with Information Technology staff to ensure that you are running the best authentication protocols you can.

Okay, great. We have a lot more technical jargon cluttering up our heads now, but what does that actually mean? How is it useful for us in our day-to-day work especially when it comes to accepting digital student records?

It is useful to us because we can tell at a glance before we dig into the cat-keyboard clutter if this email is likely to be sent from the email it purports to be sent from. If the result says Pass for SPF, DKIM, or DMARC like in our example above, the email is likely sent from the domain it claims to have been sent from. If it reads Neutral, you will need to do some more digging. If it says Fail or Softfail instead, you should not trust the authenticity of the email and definitely do not open any attachments.

I looked at one of the emails in my spam folder that was marked as dangerous to see what kind of information it would show, and it was pretty interesting.



Original Message

Message ID	<5f751886.1c69fb81.98233.ed1bSMTPIN_ADDED_MISSING@mx.google.com>
Created at:	Wed, Sep 30, 2020 at 6:46 PM (Delivered after -51 seconds)
From:	Paypal <service@particuliers.fr>
To:	peggy@transcriptresearch.com
Subject:	Unusual activity on your PayPal account
SPF:	SOFTFAIL with IP 92.243.10.36 Learn more

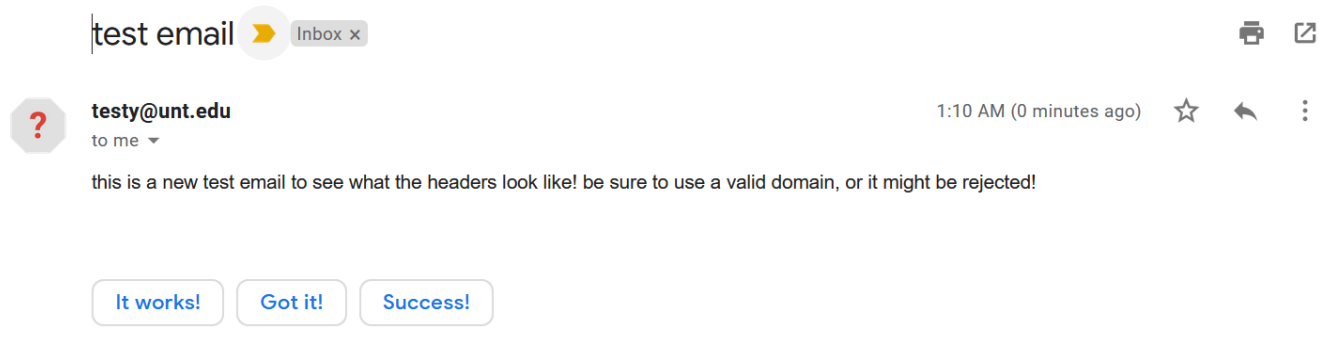
First off, I can see right off the bat that SPF was a Softfail, so I am already suspicious and ready to get more information. The email itself claims to be from PayPal and has links and logos that appear to direct to PayPal based on the URLs typed into the email, but when I hover over the links, they direct somewhere else entirely. I typically do not click on links in unsolicited emails that require me to log in somewhere that has access to any of my financial information. If I get an email claiming to be from an institutions with whom I have an account, I simply log directly into that account from my own safe link so I do not know where these links actually went.

So now that I am suspicious about this appropriately marked dangerous email, I want to look in the more detailed information. Googling the email address, I found a ton of other people who had reported this email address as an online scan that has been running for at least five years.



```
Delivered-To: peggy@transcriptresearch.com
Received: by 2002:a17:90a:890a:0:0:0 with SMTP id u10csp1397545pjn;
  Wed, 30 Sep 2020 16:45:11 -0700 (PDT)
X-Goog-Smtp-Source: ABdhPJyX77H0Ej9rKlxAxryg8cjOhJl6HQTFQQYqXJ6P+HTEB0QepHb+wdduBj4Gwi7KK/Gw/QdM
X-Received: by 2002:a50:9b5e:: with SMTP id a30mr5296508edj.49.1601509510914;
  Wed, 30 Sep 2020 16:45:10 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1601509510; cv=none;
  d=google.com; s=arc-20160816;
  b=pReYmISqC6/xb7nXmbecRRsd58migs09ImTt88sj2cmPleVPpqsPAae/UM72QoHWN1
  DNzeVO4o5TDr209+gt+1TXcsqHAtbpRNDMIyhZGmP7FunY54wPkZ8sk9UoD6dTvhL8vt
  FX93fj87Dmp50sPKsZKh+qcZkPMPGUov7CLCH8hCR/CDEqvFiuRwr48qrrflpaHQh/Aq
  CuvDAGIXmKlzHdE6W+t74HTJZdjl+J3Cm3ysr/vLq7ky4oPoWy7yGLvE27+dC56ygIS6
  /rwMgpoBkcsqURqJogiE5mnpulcXlMH4KcHYFPAeXGlrGtTtSRL+abtHxSXhbB0R39ouO
  hfTg==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
  h=date:from:to:subject:mime-version:message-id;
  bh=gGfnR07AIPDlhRaqT4DegbhPVxdPcRz4esboBYlx4mQ=;
  b=PFB1Q4i9GSmhZpqbLm2k7bmCW3adTUC6dEEfjU6bXiVjDJiCoqP55U/ZY5OoS1EU7u
  gnaiiIT81H/enfUf3AlCeHg9LUOrawyO6K67e99PfWbE4Tr73qJSueemrLoekcYYKYZ
  kamHsctw5BFGopYygbjx07S7Cpolp9ytHCw6fywOMTF9iPrtYa/FkuSXoRomK7xl6L8j
  bFACx/jgZ438nmn/Ciye84UZTRNNnkRmiXsXZ/CgxS0A0qtvYXpxwdcK76mzXZ+GRA/K
  6wpKXiXOq+luPxmDsPqעד6r0XKljn5k2R4sjaFwtVLSRGZJjRca2PQ7+9AdV2XUMIf1
  5ZZg==
ARC-Authentication-Results: i=1; mx.google.com;
  spf=softfail (google.com: domain of transitioning service@particuliers.fr does not designate
  92.243.10.36 as permitted sender) smtp.mailfrom=service@particuliers.fr
Return-Path: <service@particuliers.fr>
Received: from zealous-mcclintock.92-243-10-36.plesk.page (xvm-10-36.dc0.ghst.net. [92.243.10.36])
  by mx.google.com with ESMTPS id a3si2609437ejd.238.2020.09.30.16.45.10
  for <peggy@transcriptresearch.com>
  (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
```

In addition to using the nifty Messageheader tool, you can also investigate the headers yourself. To show how that works, I have sent myself a spoofed email using one of the spoof providers I will talk about later in this publication. Gmail nicely flagged my spoofed email with a red question mark but otherwise does not identify it as anything special.



When I entered the information on the spoof website, I set my “From” name as Testy McTester, as you can see in the next screenshot. I initially had sent my email from testy@mctesty.com, but mctesty is not a real domain name so the email did not make it to my inbox at all. Once I sent it from a fake, spoofed email address at a real domain, the email arrived in just a few seconds.



test email ➤ Inbox x



testy@unt.edu

to me ▾

this is

```
from: Testy McTester <testy@unt.edu>
reply-to: testy@unt.edu
to: peggy@transcriptresearch.com
date: Oct 30, 2020, 1:10 AM
subject: test email
security:  Standard encryption (TLS) Learn more
➤: Important according to Google magic.
```

e a valid domain, or it m

It v

We want to make sure that the “From” email address matches the display name. In this case, it does, but that is because I made a fake display name to go with my fake email address on the spoof site.

Once we start digging into the email, we can see pretty quickly that things are not looking good. That domain (unt.edu) utilizes both SPF and DMARC authentication, and my spoofed email failed on both counts. I do not need to even look any further, but let us explore more in case we get some of those more ambiguous Neutral or Soft Fail results.

Message ID	<20201030061020.E521C279C7@localhost>
Created at:	Fri, Oct 30, 2020 at 1:10 AM (Delivered after 1 second)
From:	Testy McTester <testy@unt.edu>
To:	peggy@transcriptresearch.com
Subject:	test email
SPF:	FAIL with IP 93.99.104.210 Learn more
DMARC:	'FAIL' Learn more



Even though we have these easy to identify FAILs, I still want to explore more so that I know a bit more about what I am looking at so I can feel more confident when getting digital documents.

```
Delivered-To: peggy@transcriptresearch.com
Received: by 2002:a17:90a:2:0:0:0 with SMTP id 2csp1315989pja;
  Thu, 29 Oct 2020 23:10:22 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJzvcyKli6eYi66rVQfgK9RTqM9c/Ey7/sz57Jjb2ZCJNYmDkHiq0tSrh81/+hT5BZQR22g6
X-Received: by 2002:a17:906:b010:: with SMTP id v16mr951547ejy.163.1604038221884;
  Thu, 29 Oct 2020 23:10:21 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1604038221; cv=none;
  d=google.com; s=arc-20160816;
  b=sQ/fArX6lGwKcrh7sbkK49I54u8XnZJvKIEqRQHeiuajx+hBBWHELq2CxGelJG0b18
  gauoYUbGx3+BvHUFb6fYcGcI3ydnVgaQKytFMOYZL+7D0+kbPnjSW8dWyg+ay0my7dEv
  eYxvwlkuX7mIUr3VKpTN+4rMX9+AmlAw4ftyh4OT5apklIfQuMv0kIuPLvRY6Zzj2umk
  QMx9WSJjFLY3J7JZxx83riYTkywpFABI064JOQpXaMgyeKY7mE4rq1Us0dm3nh78Q+J
  6LEvfoJskUwghYQ3txAabdGmjA8mlJOPxDvb2aYnM/vF+o1pnwD5E4e2duz6fDQwJvaL
  i/mA==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
  h=date:message-id:reply-to:errors-to:importance:from:subject:to;
  bh=/4TCv+ZQsAKcUFMvwzLb/k2r5NTb0ikRRbBnblrx+ug=;
  b=vjN/nImx60d5jsvibXCKlcfVIgD0PCxo/hCUHqWpYB3I5HKuH7jwLTonbTq0Tf7b+a
  idNsXfsohRdw9qVNNRqIUqNENAAvCeCwkAVn84rc7AMgiGOh3RxsKsmleTrQsI8QPMN/
  NVjJ4wBS8aPzZnb9avfsz33LDP64ZLtgX4hKJuoMT/FmdzqRoCbc0iUXDw9EEvkQbKKE
  XX4i20lQdY192yTbkzaNGE0uoLkX35+8IU0iKAUi00nKO9JXIQ89i3A7wMeSZPWOxTEJ
  0VeuAYqLiNlmWBEPi9iW41YfwhAFwzaG0UGF8muyizoRYNCZ8E0LDNDNAFr9Os9RIBf
  DNUw==
ARC-Authentication-Results: i=1; mx.google.com;
  spf=fail (google.com: domain of testy@unt.edu does not designate 93.99.104.210 as permitted sender)
  smtp.mailfrom=testy@unt.edu;
  dmarc=fail (p=NONE sp=NONE dis=NONE) header.from=unt.edu
Return-Path: <testy@unt.edu>
Received: from localhost (emkei.cz. [93.99.104.210])
  by mx.google.com with ESMTPS id b18si4875437edh.71.2020.10.29.23.10.21
  for <peggy@transcriptresearch.com>
  (version=TLS1_2 cipher=ECDHE-ECDSA-CHACHA20-POLY1305 bits=256/256);
  Thu, 29 Oct 2020 23:10:21 -0700 (PDT)
Received-SPF: fail (google.com: domain of testy@unt.edu does not designate 93.99.104.210 as permitted sender)
client-ip=93.99.104.210;
Authentication-Results: mx.google.com;
  spf=fail (google.com: domain of testy@unt.edu does not designate 93.99.104.210 as permitted sender)
  smtp.mailfrom=testy@unt.edu;
  dmarc=fail (p=NONE sp=NONE dis=NONE) header.from=unt.edu
Received: by localhost (Postfix, from userid 33) id E521C279C7; Fri, 30 Oct 2020 02:10:20 -0400 (EDT)
To: peggy@transcriptresearch.com
Subject: test email
```

Let's look at each of these highlighted elements in more detail.

```
ARC-Authentication-Results: i=1; mx.google.com;
  spf=fail (google.com: domain of testy@unt.edu does not designate
93.99.104.210 as permitted sender) smtp.mailfrom=testy@unt.edu;
  dmarc=fail (p=NONE sp=NONE dis=NONE) header.from=unt.edu
```

First up, we see that the domain (in this case, unt.edu) does not designate this IP address as a permitted sender. This is why we got the overall DMARC Fail, which is listed next to the DMARC box in the table but also in the detailed headers itself.

Next up, we are going to look at the Receiver information to see if that matches up.



Return-Path: <testy@unt.edu>
Received: from localhost (emkei.cz. [93.99.104.210])

This is pretty important! Looking at the “Received: from” segment, we can see that this supposedly US-based email was sent by a server in the Czech Republic. If we compare that with our first sample from CHESICC in China, we can see the Received: from domain is qq.com, also in China. This is not always a perfect match, but it is another data point to consider. Emkei.cz is a very popular spoof website and one that you definitely want to watch out for because there is no legitimate reason for an educational institution – even in the Czech Republic – to be sending their documents via Emkei.cz.

Received-SPF: fail (google.com: domain of testy@unt.edu does not designate 93.99.104.210 as permitted sender) client-ip=93.99.104.210;
Authentication-Results: mx.google.com;
 spf=fail (google.com: domain of testy@unt.edu does not designate 93.99.104.210 as permitted sender) smtp.mailfrom=testy@unt.edu;
 dmarc=fail (p=NONE sp=NONE dis=NONE) header.from=unt.edu

And then we get more confirmation that DMARC failed because this IP address is not authorized to send emails from this domain.

What happens if we plug this information into the Google Admin Toolbox? It is simply a cleaner and shorter way of telling us the same thing; honestly, the trickiest part is remembering the website address.

Google Admin Toolbox Messageheader

MessageId	20201030061020.E521C279C7@localhost
Created at:	10/30/2020, 1:10:20 AM CDT (Delivered after 2 sec)
From:	Testy McTester <testy@unt.edu>
To:	peggy@transcriptresearch.com
Subject:	test email
SPF:	fail
DMARC:	fail

#	Delay	From *	To *	Protocol	Time received
0	1 sec	emkei.cz. →	[Google] mx.google.com	ESMTPS	10/30/2020, 1:10:21 AM CDT
1		→	[Google] 2002:a17:906:b010::	SMTP	10/30/2020, 1:10:21 AM CDT
2	1 sec	→	[Google] 2002:a17:90a:2:0:0:0	SMTP	10/30/2020, 1:10:22 AM CDT



If you are using an external email client, you may need to speak with someone at your institution to have them show you how to check email headers in your email service.

Why do we go to all this work? Is this really a big deal? According to some of the many articles I read while trying to prepare this information, approximately 1 in 4 emails purporting to be sent from a US .gov email address is fake. There are reports that impersonation email attacks are the fastest growing email-based cyber attacks, and that scammers are sending over 3 billion domain spoofing emails a day, costing billions of dollars in the last half dozen years in the United States alone.

It is also very easy to send anonymous or spoofed emails or prank emails from websites like Emkei's Fake Mailer (the spoof website I used for this example), Fake Mail Generator, Anonymailer, Dead Fake, Send Anonymous Mail, and many others. There are also temporary email services like Guerrilla Mail or ProtonMail that let you create a temporary, anonymous email account to both send and receive emails, but they do not allow spoofing of email addresses. If you are not already checking detailed header information, you really should.

Checking the detailed headers will only tell you limited information if the email address has been spoofed. If it is a legitimate email address that is only pretending to belong to an authentic source, this research will not help identify that. For example, if someone creates a real gmail account such as YourInternationalSchool123@gmail.com, and pretends that this newly created email address belongs to the school and sends you falsified documents, the detailed headers will still only give you limited information. The SPF, DKIM, and DMARC would likely pass in this made-up example if I created such an email address since I could legitimately send email from that address. That does not mean that the email address is legitimately associated with that institution, only that the email address itself is real. If I create that gmail account, it is a real account, just not associated with the school.

What do you do if the email address seems to be legitimate, but you are unsure if you can trust it, especially if it comes from a free email service provider? We regularly see authentic emails from gmail, yahoo, and other web-based mail accounts that are being used by secondary, vocational and higher education institutions, examination boards, and even ministries of education. A branded email account is when the email address matches the website's domain, so that the email address usually has name@domain.com. Institutions may use these non-branded email accounts for a variety of reasons.

Branded emails have a fee associated with them and require more skill to set up. Maybe they have had several website domain changes tied to whoever is in power and want to continue to use the same email address regardless of the outcome of the next election. Perhaps their country's internet infrastructure is not as reliable as they would like, or they want to be able to access their email remotely. Perhaps the former administrator of the domain-branded email account left the institution and did not share the password. Maybe they prefer the convenience of having a free email service that can be transferred to a new website if their current website is not renewed due to budget cuts. Perhaps they like creating a new generic email addresses for each new admissions classes such as School123-2020@gmail.com and School123-2021@gmail.com. There are a whole host of legitimate reasons for educational institutions and educational authorities to use web-based email providers. However, that certainly makes it more difficult to identify if that email address is truly used by the institution that appears to be sending you official documents, or if a student created a fake email address and is pretending to send you documents on behalf of a school they might have never even attended.



That is when we have to put our research skills to work. Generally, we try to look up email addresses that are unknown to us by typing the email address into a search engine in quotes and see what that brings up, like “YourInternationalSchool123@gmail.com”. In the majority of situations, we are able to find that email address listed on the institution’s website, a government website, or some other reliable source that makes us feel good about accepting it even though it is not domain branded. Other times, though, we find a website for the institution, and they have an entirely separate email address. In those cases, we send an email to those publicly-shared addresses and ask about the legitimacy of both the email address and the documents and update our internal database when we get a response.

I do want to point out that there have been cases where unscrupulous companies have cloned legitimate verification websites in appearance and put their falsified URL on falsified documents. We have also received inauthentic documents with QR codes that have lead to fraudulent websites such as the fake CHESICC website which pretended to verify falsified documents or to websites totally unrelated to education or educational records. If you are using a website or email address that is printed on the digital documents, make sure that you are able to independently confirm the validity of that email address or the main website address. If you are accessing a portal that is listed on the documents, ensure that you can navigate to that same link from the institution’s official website.

We also check with our resources. TAICEP, The Association for International Credential Evaluation Professionals, maintains a database of more than 3000 verification resources, ranging from email addresses to postal addresses to online portals maintained by the Resources for Members Committee. TAICEP has also designated a task force on Digital Student Data to provide even more resources and guidance regarding digital student data and electronic verification tools. This task force disseminates information about pan-institutional databases through presentations and newsletter articles and is working on a global mapping tool. Other membership organizations also have country- and regional-experts who may be able to assist you in finding other contacts or verifying email addresses.

Essentially, you only want to accept digital documents from verified senders from trusted sources or direct relationships. Unfortunately, there are times when we are not able to find a reliable looking website or electronic contact information. In those situations, we try to send documents by mail, and we reach out to colleagues in the field and to contacts in-country. EducationUSA has been an invaluable resource, and they are often able to reach out to local institutions to ask questions for us, often providing us with contact information or communicating with a local school in our stead. Similarly, we have contacted ENIC-NARIC Network offices for assistance in European countries. We reach out directly to the Ministry of Education or other educational authorities in the country.

Ultimately, though, if we are unable to verify the validity of an email address, we are simply unable to accept digital documents sent from that email address. On our website and our application from, we make that clear. “For electronic records, we must be able to confirm that the sender is the appropriate authority at the institution that issues educational records. If we are unable to verify that the email address sending us the documents is the person or office authorized to issue the records (controller of exams, registrar, records office, etc), then we will not be able to accept the electronic records and will require official documents as specified above.”

By making our requirements and expectations clear up front, we are able to reject the emailed documents if we are not confident in their provenance. We can accept a wide variety of digital records,



but we are still protecting the validity of our evaluation reports by doing our due diligence to ensure that the documents we receive are sent by the appropriate authority.

Types of Emails

Sometimes we get emails from the learner or from the institution that direct us to the institution's portal to download the official academic records. There are really two major types of emails that have attachments: secure emails and plain emails.

Secure or encrypted emails have been encoded so that email messages cannot be intercepted and read by anyone other than the sender and recipient. This can be done either encrypting an email while it is in transit (known as Transport Layer Security or TLS) or through end-to-end encryption. Both TLS and end-to-end encryption require additional work on behalf of both the sender's and receiver's email clients because both have to be set up on the same form of encryption for the email to be received and readable. Many higher education institutions work around this complication by sending links to their digital portals with a separate email that has a security code that allows you access to the portal.

TLS is the most common and most basic form of email encryption and is the default form of encryption used by some of the most popular email providers like Gmail and Microsoft for sending secure email. With TLS, both the sender and receiver must be set up for TLS in order to ensure a secure connection, which is one challenge. Another challenge is that TLS is only providing encryption on the transmission channel, not the data that is being transmitted.

To send an encrypted email, the sender has to set up an account with an encryption application such as Proton Mail, Send 2.0, Enlocked, Microsoft 365, or others. Some of these work with web-based email clients such as Gmail or Yahoo, while others work only on one product like Microsoft 365 Message Encryption for Outlook.

As a very, very non-technical description, encrypting an email means that it is converted from plain text to a jumble of indecipherable characters. The recipient must have the private encryption key to match the public key in order to be able to read the email; that means that both the sender and receiver are using email products that support that type of encryption. In addition, the recipient has to have the key in order to be able to read the locked/encrypted email. When you enter a recipient's information in the "to" field, your email client will check to see if you have already sent the encryption key to the recipient so that they can read your email. Some email services such as Outlook offer an easy way to send encrypted emails by having an Encrypt button or changing security settings to turn on encryption. Generally speaking, this can be done on a case-by-case basis or as a default for all emails.

Gmail automatically encrypts all emails via TLS. Gmail also supports S/MIME (Secure/Multipurpose Internet Mail Extensions), an advanced encryption that encrypts the message itself, not just the digital envelope. S/MIME support is only available for some of its G Suite account types. Outlook also encrypts emails while they are in transit via TLS, but Microsoft also created its own encryption standard. Yahoo protects your messages while in transit, but you need to use a plug-in for end-to-end encryption. If your institution is using a branded email provider, you will want to check with your IT staff to find out about the type of encryption your institution is using.



Institutions can also send password-protected email as another mechanism for protecting email, and we will talk a bit more about that in the next section. In addition, some institutions that sent documents via plain text also have an online tool for verification of some or all information. This document is not focused on verification, though my organization has done quite a lot of work in that arena. Please feel free to check out our website for some of our many conference handouts on the topic.

Many of us are receiving digital documents primarily via plain email. Only you can determine if the information in this document and other resources will help you feel comfortable accepting plain emails. You have to look at your institution's policies regarding electronic documentation, which may prohibit you from accepting plain emails that have student records attached unless there is some other kind of security feature in place. Whatever you decide, it is best to have a documented policy to share with your coworkers and students to remove the uncertainty and to make sure everyone knows what it is expected and accepted.

Also, if your institution is suddenly accepting more digital documents than you were before, be sure to regularly check your spam folder. In addition, you will want to download an attachment and then check it against your computer's anti-malware product before you open it, even if your email provider also scans incoming messages for malware and other threats.

Types of Attachments

We receive emails with all sorts of attachments, from image files to word processing documents to PDFs (Portable Document Formats). It is fairly common for institutions to scan or photograph the official documents and send that as image file; .jpg, .bmp, or .gif are the most common types we see. We are generally willing to accept those emails, though only if they are attachments and not URLs that appear to be directing us to an image file. We also occasionally receive transcripts, especially for secondary school records or translations, that were created in a word processor or spreadsheet program, with extensions .doc and .xls being the most common. At my institution, we do not accept word processing files from institutions because of the security vulnerabilities, so we require the institution to convert the attachment to a PDF. We definitely do not accept executable (.exe), compressed (.gz or .bz2), or zipped (.7zip or .zip) files, so on the rare occasions that we receive them, we immediately delete them without opening them and let the student or institution know that our company policy prevents us from accepting those documents.

Sometimes the emails we get will direct us to an online portal. This is a website that has some kind of proprietary information. This may include insecure portals without login information such as the examination board websites we mentioned earlier that do not require a login to access data. In those situations, you are able to access the data to verify it by entering information directly off of the document into the online portal. That way, random people are generally not able to access everyone's information, but even that possibility is considered a low threat since many countries report examination scores on the local radio or post them in the newspapers.

Other portals may require an account with a username and password. In those scenarios, the email you receive may direct you on how to create an account because the portal's owner wants to be able to limit access to the data to those who would need it in their business. This is fairly common in education; the



provider of the data wants to limit its access to students, educators, and those in related fields. These types of portal systems allow long-term access to the portal as well as access to large numbers of Examples of this type of portal include the Higher Education Degree Datacheck (HEDD) and the CIE Direct online tool from Cambridge International Education. In the former example, third parties must submit a signed released form from the learner and pay a fee to verify the learner's graduation document. In the latter, third parties apply to Cambridge Assessments to confirm that they are relevant professionals who would have a reasonable need to access Cambridge examination results. In both cases, the user must log in to their own approved institutional account and then enter information from student's records.

Alternately, institutions may send you an email with access to retrieve a specific student's records, often for a limited time or limited number of logins. The learner herself needed to grant access to your email address to be able to view and download her official student records. In this manner, the institution allows the student learner to limit who has access to her records and for how long. This also allows the institution to limit access to their entire system because third parties are not logging in individually to verify any number of records for whom they have unofficial documents; in this scenario, the student learner maintains control over who has access to her information. The third party receiving this information only has access for however long the student and the institution approve and cannot access another student's records without that student also going through the process to have the institution send a new email to your email address granting access. Some portals of this type, such as ETX-Nigeria do allow institutions to create a 'receiver' account to make it easier for large numbers of students to digitally release their records to your institution in a standardized way.

Some of these types of portals will send you a unique URL that can only be used by your email address to access that student's records for a limited other. Other emails from institutions may have a follow-up email with the password required to access the institutional portal. The follow-up email may come automatically once the institution receives a digital notification that you have read the email, or it may come after you go to the website in the email and request a password or passcode, which is automatically sent to your email address. Sometimes, the same third-party provider may offer their institutional users a variety of options so one institution may have a different mechanism for downloading the official student records than another institution using the same provider.

And those third-party providers may also have additional layers of security, including 2-step authentication or 2-factor authentication (2FA). Multi-step or multi-factor authentication requires a combination of security features. One of the most common methods is combining a password entered in a portal followed by a code sent to your registered phone number by text message or through an external authenticator application such as Authy or Google Authenticator.

Security Features

We have already talked a bit about the security features in email configuration as we all secure emails that require a password to even open the email. Another popular security feature that requires the least technical ability is securing the documents that are being sent electronically. It is fairly common for institutions to refuse to accept digital documents unless the sending institution uses email encryption or only sends secure documents. Two main methods for doing this are securing an attachment and using a document sharing platform.



Password protecting a PDF is pretty straightforward. Depending on the PDF program you are using, you may be able to find the password setting in Tools > Protect or something similar. Some PDF programs require you to have a paid account in order to be able to password-protect the document while others simply require you to create a login account on their website. It is not much different when password protecting a document such as a word processing document or spreadsheet. Most stand-alone word processing or database document providers have the option to easily adjust the properties of a document to add the protection of a password. The sending institution would need to password protect the document before sending it to you and also separately provide you with the password so you can open the attachment. Sometimes this is handled by the institution sending the document and the student sending the password. We have also seen cases where an automatic email provides a randomly generated password after sending the attachment.

A document sharing platform allows people to send digital documents via the internet through a cloud service. These have become increasingly popular over the last decade and include such popular names as Google Drive, OneHub, Dropbox, Microsoft One Drive, Box, and others. While most cloud services have security that prevents outsiders from accessing their documents, these file sharing services generally also allow individual files to be shared to specific email addresses. That way, only the designated recipient is able to view and/or download the documents. In addition, some institutions may take it a step further and share password protected documents via cloud access but also require a password or passcode that was sent separately.

There are also third-party products such as Digify or DocSend that allow you to secure your email and digital documents but also go a step further by setting watermarks, setting documents to expire automatically, revoking access to electronic documents, and even unsending emails.

Certified Documents

Another tool for increasing confidence in the authenticity of documents is Adobe Certified Document Services (CDS). When an educational institution signs their digital academic records using the CDS, this means that the documents have been digital signed by a trusted Certificate Authority. When the PDF is opened using recent versions of Adobe Reader or Adobe Acrobat, it electronically validate the digital signatures without requiring any additional software or hardware. This allows the educational institution to issue electronic transcripts to disparate recipients while ensuring the authenticity of the documents. As seen on the image below, there will be a blue bar across the top that shows that the transcript is Certified, by whom, and what CDS was used.





When the document is opened using Adobe, the bar across the top will reflect one of these three states: valid, invalid, or validity unknown. The blue ribbon means that the digital certificate is valid, while a red x indicates that you should not trust the validity of the document. If the validity of the author is unknown, you may need to take some additional steps, including making sure you are connected to the internet. You may need to contact the institution if the document seems to be authentic but has mixed messages regarding the validity.



Document Is Valid



Validity Unknown



Document Is Invalid

I have expanded this transcript below by clicking on the Signature Panel button to bring up the sidebar on the left and then widening that sidebar to make it easier to see.

The screenshot shows a PDF document viewer interface. On the left, a sidebar titled 'Signatures' is expanded, displaying details for a signature: 'Certified by Parchment', 'Valid certified document', 'Source of Trust obtained from Adobe Approved Trust List (AATL)', 'Changes have been made to this document that are permitted by the certifying party', 'Signer's identity is valid', 'The signature includes an embedded timestamp.', 'Signature is LTV enabled', and 'Signature Details' with a timestamp of '2020:10:06 16:55:39 -05'00' and the field name 'ParchmentSig1 (invisible signature)'. The main content area displays the University of Toronto logo and 'ENROLMENT SERVICES' contact information (172 St. George Street, Toronto, Ontario, Canada M5R 0A3). Below this is a section titled 'How to Authenticate This Official PDF Transcript' with three paragraphs of text explaining the document's electronic transmission and digital signing. The first paragraph states the document is for the recipient's use only. The second paragraph explains the digital signature process and the blue ribbon symbol. The third paragraph explains the 'Invalid' status, which could mean the document is not authentic, has been altered, or the signature has expired. The fourth paragraph explains the 'Author Unknown' status, which could mean the certificate is self-signed or issued by an unknown authority.

Certified by Parchment. Parchment, certificate issued by GlobalSign CA 5 for AATL. Signature Panel

Signatures ×

Validate All

✓ Certified by Parchment

Only form fill-in, signing and page adding actions are allowed

Valid certified document:

Source of Trust obtained from Adobe Approved Trust List (AATL).

Changes have been made to this document that are permitted by the certifying party

Signer's identity is valid

The signature includes an embedded timestamp.

Signature is LTV enabled

Signature Details

Last Checked: 2020:10:06 16:55:39 -05'00'

Field: ParchmentSig1 (invisible signature)


UNIVERSITY OF TORONTO


ENROLMENT SERVICES
172 St. George Street
Toronto, Ontario, Canada
M5R 0A3


How to Authenticate This Official PDF Transcript

This official PDF transcript has been transmitted electronically to the recipient, and is intended solely for use by that recipient. It is not permissible to replicate this document or forward it to any person or organization other than the identified recipient. Release of this record or disclosure of its contents to any third party without written consent of the record owner is prohibited.

This official transcript has been digitally signed and therefore contains special characteristics. This document will reveal a digital certificate that has been applied to the transcript, and for optimal results, we recommend that this document is viewed with the latest version of Adobe® Acrobat or Adobe® Reader. This digital certificate will appear in a pop-up screen or status bar on the document, display a blue ribbon, and declare that the document was certified by the University of Toronto, with a valid certificate issued by GlobalSign CA for Adobe®. This document certification can be validated by clicking on the Signature Properties of the document.

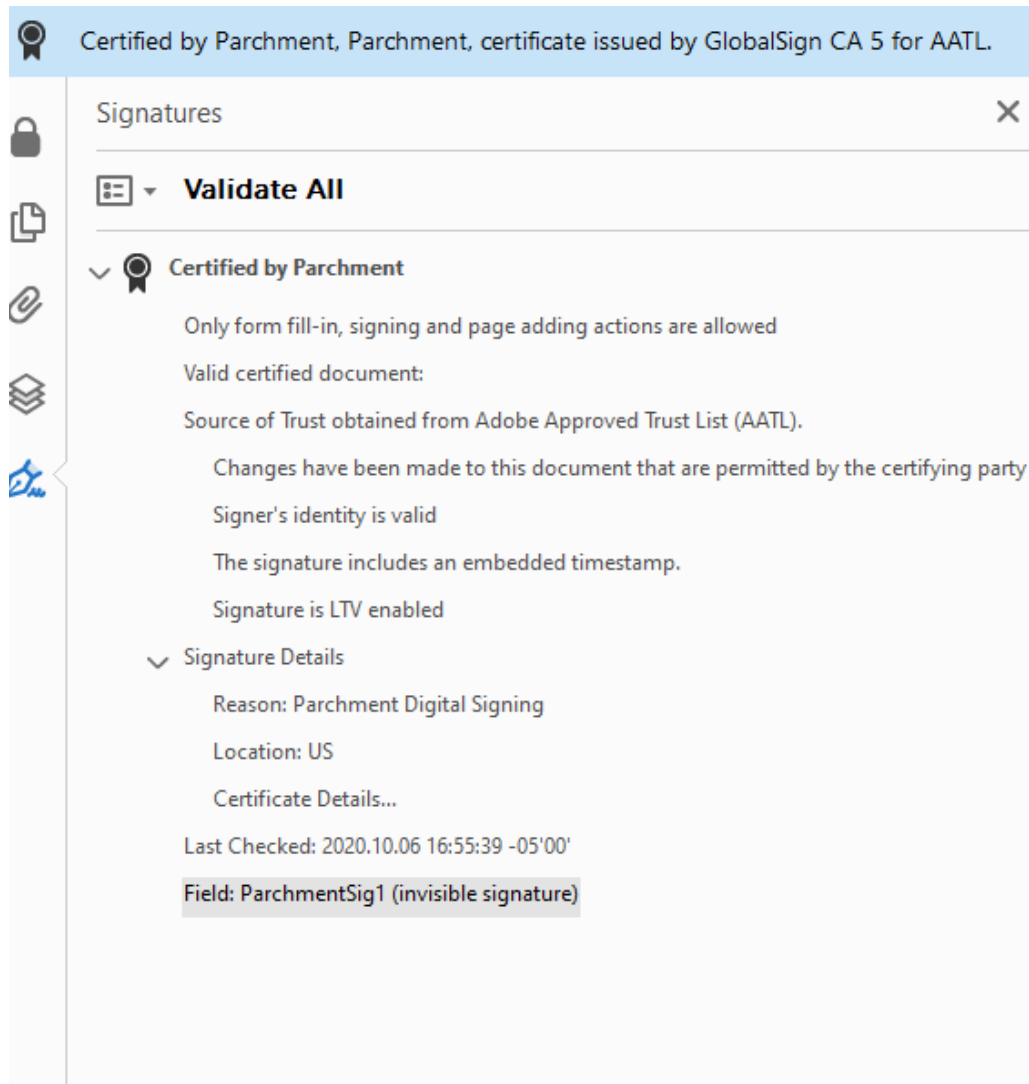
 **The Blue Ribbon Symbol:** The blue ribbon is your assurance that the digital certificate is valid, the document is authentic, and the contents of the transcript have not been altered.

 **Invalid:** If the transcript does not display a valid certification and signature message, reject this transcript immediately. An invalid digital certificate display means either the digital signature is not authentic, or the document has been altered. The digital signature can also be revoked by the transcript office if there is cause, and digital signatures can expire. A document with an invalid digital signature display should be rejected.

 **Author Unknown:** Lastly, one other possible message, Author Unknown, can have two possible meanings: The certificate is a self-signed certificate or has been issued by an unknown or untrusted certificate authority and therefore has not been trusted, or the revocation check could not complete. If you receive this message make sure you are properly connected to the internet. If you have a connection and you still cannot validate the digital certificate on-line, reject this document.



Here is a close-up view of the Signature Panel:



The blue Certified bar shows that this particular transcript is certified by Parchment, signed by Parchment, and the trusted certificate was issued by GlobalSign. GlobalSign is one of several companies, including VeriSign and Entrust, that issues official digital transcripts using Adobe's Certified Document Services. Since it has the blue ribbon, that means it is a valid signature, and you can see the details of the signatory and other information in the image.

Universities around the world may issue their official digital transcripts via one of these Adobe document services, helping to increase confidence in the document.





“The digital signature provides a tamper-evident wrapper on the document. The blue ribbon seal must be present to both authenticate and demonstrate the integrity of the document. This is automatically verified when the recipient views the authentic document using the free Adobe® Reader.”



If you are uncertain about accepting PDF transcripts as official, you can also check the institution's website to see if there is any information. Many higher education institutions have updated their transcript order or registrar web pages to explain their digital document security practices, especially since so many are currently unable to send original documents by post due to school closures and distance learning measures imposed due to the pandemic.

Transcripts sent via National Student Clearinghouse, Parchment, and Digitary that we have received have all been issued with the Adobe CDS tool.


Certified by Certified Document Services <cds@studentclearinghouse.org>, National Student Clearinghouse, certificate issued by GlobalSign CA 3 for AATL.

CARLOS ALBIZU UNIVERSITY

OFFICIAL ACADEMIC TRANSCRIPT

P.O. Box 9023711
San Juan, PR 00902-3711
Tel. (787) 725-6500





Official eTranscript Page: 1 of 1 Printed on: January 12 2018

Please note that many of the documents we have received via these third party providers such as Parchment and Digitary have indicated that “At least one signature is invalid.” When looking at the details, we can see that it does not list who has certified and signed the document; instead, we see “Certified by %s” instead of Parchment, Digitary, or whomever issued the document.

At least one signature is invalid.

Signatures

 **Validate All**

 **Certified by %s**


Only form fill-in, signing and page adding actions are allowed

Signature is invalid:

There are errors in the formatting or information contained in this signature (support information: SigDict/Contents illegal data)

Signer's identity has not yet been verified

Signing time is from the clock on the signer's computer.

 **Signature Details**


Reason: Document Certification

Location: Dublin, Ireland

Certificate Details...

Last Checked: 2020.10.06 19:14:57 -05'00'

Field: Signature1 (invisible signature)

 **Rev. 2: Signed by Unknown**

Signature is invalid:


There are errors in the formatting or information contained in this signature (support information: SigDict/Contents illegal data)

Signer's identity has not yet been verified

Signature is a document timestamp signature.

Last Checked: 2020.10.06 19:14:57 -05'00'

Field: Signature2 (invisible signature)



University of Newcastle upon Tyne

Faculty of Humanities and Social Sciences



Since we are receiving these documents directly from those third party services, who only accept the transcripts directly from the higher education institutions, we assume it is a disconnect between whose security signature has been transmitted: the institution's or the third party digital repository's.

If you are currently examining your digital documentation processes in response to the global pandemic that has shuttered and distanced educational institutions around the world or have been accepting digital documents for a while, it is best to have these types of conversations before you have a frantic student begging for your help.