Court File No.: A-102-20

FEDERAL COURT OF APPEAL

BETWEEN:

AIR PASSENGER RIGHTS

Applicant

– and –

ATTORNEY GENERAL OF CANADA

Respondent

– and –

CANADIAN TRANSPORTATION AGENCY

Intervener

SUPPLEMENTARY AFFIDAVIT OF DR. GÁBOR LUKÁCS
(Affirmed: November 29, 2022)

I, **DR. GÁBOR LUKÁCS**, of the City of Halifax in the Province of Nova Scotia, AFFIRM THAT:

1. I am the President and a Director of the Applicant, Air Passenger Rights. As such, I have personal knowledge of the matters to which I depose, except as to those matters stated to be on information and belief, which I believe to be true.

2. A copy of the document entitled "Entrust S/MIME Solution FAQs," retrieved from https://www.entrust.com/-/media/documentation/faqs/smime-fq.pdf, from Entrust's website, is attached and marked as **Exhibit "A"**.

3. According to Exhibit "A":

> **As an IT administrator, can I recover an employee's private key if it becomes lost or the employee leaves the organization?**
>
> **Yes.** The Entrust S/MIME solution includes a Key Escrow Module that enables authorized third parties to recover stored keys to

> decrypt data and enable security and compliance requirements. The private key of each end-user remains on the device and is non-exportable. However, during the deployment process the private key is escrowed to an encrypted file format that can be integrated with an HSM if required. This also prevents employees from potentially extracting the private key from the system and saving it for their own use after leaving the organization.

4. An excerpt of Entrust's "Certification Solutions FAQ" page, containing the section entitled "Secure Email Certificates," is attached and marked as **Exhibit "B"**.

5. According to Exhibit "B":

> The keys are stored in Entrust's secure facility, protected by a security level that no one customer would be able to provide on their own; it is the same protection offered by our public certificate business. They have the same level of protection as our CA keys, including aspects of physical security (room access), logical security (dual custody for access) and storage security (encrypted and integrity-protected with CA keys) This is not a case of any Entrust IT employee could get at these.

AFFIRMED remotely by Dr. Gábor Lukács at the City of Halifax, Nova Scotia before me at the City of Coquitlam, British Columbia on November 29, 2022, in accordance with O. Reg. 431/20, *Administering Oath or Declaration Remotely*.

Dr. Gábor Lukács

Halifax, NS
Tel:
lukacs@AirPassengerRights.ca

Commissioner for Taking Affidavits

Simon (Pak Hei) Lin, *Barrister & Solicitor*
LSO #: 76433W
4388 Still Creek Drive, Suite 237
Burnaby, BC V5C 6C6

CERTIFICATE OF COMMISSIONER FOR TAKING AFFIDAVITS

I, Simon Lin, a Commissioner for taking Affidavits in Ontario, certify that:

1. This certificate is provided in accordance with the *COVID-19 Notice No. 2* of the Supreme Court of British Columbia.

2. On November 29, 2022, I commissioned the Affidavit of Dr. Gábor Lukács [**Deponent**] in this matter [**Affidavit**]. The Affidavit was commissioned remotely using video technology and a secure electronic signature platform, as permitted by the Law Society of Ontario and O. Reg. 431/20, *Administering Oath or Declaration Remotely*.

3. I was satisfied that the process was necessary because it was medically unsafe, for reasons associated with COVID-19, for the Deponent and a commissioner to be physically present together.

4. The Affidavit was loaded in PDF format by the commissioner onto a secure electronic signature platform, which:

    a. does not permit the Deponent to add or remove any of the pages;

    b. required both the commissioner and Deponent to apply their initials on each page of the Affidavit; and

    c. required both the commissioner and Deponent to apply their electronic signatures where a signature is required.

5. The Deponent was emailed a link to the platform to securely sign the Affidavit, Thereafter, the following process was followed while the commissioner and Deponent was connected via video technology:

    a. The Deponent showed me the front and back of the Deponent's current government-issued photo identification [**ID**], which I have retained screenshots of.

    b. I compared the video image of the Deponent and the information on the ID and was satisfied that it was the same person.

    c. The copy of the Affidavit before the commissioner and Deponent were on the same electronic platform and are identical.

    d. I administered the oath to the Deponent who affirmed/swore to the truth of the facts in the Affidavit and the Deponent applied their electronic signature.

November 29, 2022

Signature of Simon Lin
Commisioner for Taking Affidavits

This is **Exhibit "A"** to the Affidavit of Dr. Gábor Lukács

affirmed before me on November 29, 2022

_____

Signature

Entrust S/MIME Solution FAQs

What is an S/MIME certificate?

Secure/Multipurpose Internet Mail Extension (S/MIME) certificates secure email communication through end-to-end encryption and identify the sender via a digital signature. They are a standard for public key encryption and signing of MIME data.

With S/MIME certificates, recipients of an email can identify where the email came from, so employees can verify that the email came from a CEO, CFO, or other member within the organization and can trust the "From" address of the email.

What is included in the Entrust S/MIME Certificate Solution?

When we refer to our S/MIME "solution," we are referring not just to our Entrust S/MIME certificates, but also integrated automation features from our technology partner, Sixscape Communications, including:

- **Secure Mail Module:** A security add-in for popular email clients for certificate-based digital signing and encryption of emails
- **Key Escrow Module:** Enables authorized third parties to recover stored keys to decrypt data and enable security and compliance requirements
- **Secure Large File Transfer:** Provides the end-user with the ability to securely transfer large files to intended recipients using S/MIME technology
- **Mobile Device Management Module:** Allows for delivery of keys and certificates to user's mobile device
- **Retrocrypt Module:** Provides the ability to globally or selectively encrypt legacy email in folders as well as new incoming email

Learn more about Entrust S/MIME certificates at entrust.com

Entrust S/MIME Solution FAQs

What dangers can organizations experience from email attacks?

There are two types of email hacking activities:

- **Phishing:** When generic messages are delivered to a wider pool of potential victims
- **Spear phishing or business email compromise (BEC) attacks:** Specific and planned targeted attacks to an individual or a group; these attacks aim to:
  - Extract sensitive information
  - Install malware onto the network
  - Wire money to accounts that belong to the attackers

How big of a threat are business email compromise (BEC) attacks?

BEC attacks have been exploding in recent years, moving across geographies and business sectors. According to the most recent FBI Internet Crime Reports (ICRs), organizations in the U.S. lost $6.4 billion to BEC attacks from 2014 to 2020 – with $1.8 billion of that in 2020 alone.*

What are the risks/costs associated with NOT securing emails?

The biggest risk to an organization not securing their emails is that it leaves them vulnerable to email hacking activities (mentioned earlier), which can result in theft of their intellectual and capital property as well as damage to their brand and erosion of customer trust.

There are also certain compliance risks that organizations can face depending on their sector or jurisdiction in which they do business. For example, in the U.S., the Health Insurance Portability and Accountability Act (HIPAA) requires that organizations protect sensitive patient health information from being disclosed without a patient's knowledge or consent. According to the U.S. Department of Health and Human Services, HIPAA violation costs in 2020 alone were $13 million.

In the European Union, the General Data Protection Regulation (GDPR) guidelines state that personal data must be fully protected, and if it's not, organizations can be subjected to fines of up to 4% of their preceding year's revenue or up to 20 million euros.

* FBI Internet Crime Reports 2014-2020

Entrust S/MIME Solution FAQs

How can S/MIME certificates help reduce an enterprise's attack vector?

S/MIME certificates can help reduce an enterprise's attack vector by providing:

- **Identity:** Entrust S/MIME certificates provide identity by enabling employees to digitally sign emails so recipients know that the email is coming from an employee of the organization. Emails that are digitally signed by an employee can be trusted to come from the stated source and provide assurance that the content hasn't been modified during transit.
- **End-to-end encryption:** Entrust enables employees to encrypt emails, making the theft of encrypted emails without access to the private keys useless to an attacker. Entrust's end-to-end encryption is inherently a stronger form of security compared to gateway encryption.

Why has it been difficult for organizations to deploy S/MIME certificates?

Even though email is an essential business tool and S/MIME and PKI have been around for decades, S/MIME historically has had a very low adoption rate in an enterprise context.

Some of the biggest challenges have been that S/MIME certificates are often costly and time-consuming to deploy and manage because there are many manual steps that make it hard for enterprises to scale without significant IT and employee support. Plus, many employees have multiple devices and computers, and the same S/MIME certificate needs to be installed across all of them, making the IT and employee burden even higher.

If enterprises follow best practices by encrypting their emails to protect their data, employees will get locked out of their emails (just as a bad actor would) if their private key gets lost. This requires the retrieval of those keys in a secure way and reprovisioning the employee device.

Entrust has partnered with Sixscape to provide a solution that can provide both automation and private key escrow capabilities. It "checks all of the boxes" and allows organizations to deploy to a large enterprise within seconds, minutes, and hours as opposed to days, weeks, and months.

Are Entrust S/MIME certificates easy to install?

Yes. Our centralized and decentralized one-time deployment gives network teams the ability to deploy on behalf of end-users within minutes or support a self-service end-user model, regardless of the number of users.

Does the Entrust S/MIME solution provide protection across multiple devices?

Yes. It supports a scalable deployment of email encryption and identity within your organization – across multiple devices such as desktops, laptops, tablets, and mobile phones.

Entrust S/MIME Solution FAQs

Will the Entrust S/MIME solution protect our employees from phishing emails from third parties?

Yes. By enabling S/MIME internally and externally, phishing emails can be mitigated because emails exchanged between both parties will be digitally signed. Furthermore, the digitally signed email with an Entrust certificate can be trusted by any party.

As an employee, is it possible to get a solution that can be used for both email signing and email encryption?

Yes. When requesting an S/MIME certificate on your device, you can specify signing, encryption, or dual-purpose certificates. If you need to digitally sign to support non-repudiation, choose signing certificates.

As an IT administrator, can I recover an employee's private key if it becomes lost or the employee leaves the organization?

Yes. The Entrust S/MIME solution includes a Key Escrow Module that enables authorized third parties to recover stored keys to decrypt data and enable security and compliance requirements. The private key of each end-user remains on the device and is non-exportable. However, during the deployment process the private key is escrowed to an encrypted file format that can be integrated with an HSM if required. This also prevents employees from potentially extracting the private key from the system and saving it for their own use after leaving the organization.

As an IT administrator, can I deploy email encryption and identity across multiple devices for each employee?

Yes. The Entrust S/MIME solution deploys to desktops, laptops, and corporate-issued mobile devices seamlessly by leveraging popular mobile device management (MDM) solutions. For encrypted email, employees can have the same secure email credentials (digital identity) in each of their devices used for email. The user can access their encrypted email anytime, anywhere.

Entrust S/MIME Solution FAQs

As an IT administrator, can I encrypt legacy email that is currently in the clear or incoming email that is not encrypted?

Yes. The Entrust S/MIME solution can automatically encrypt users' old, unencrypted emails with the private keys of the user's respective S/MIME certificates at time of deployment. This ensures a stronger security posture because all previous/legacy emails are signed and/or encrypted with the new certificate and private key. Furthermore, with all emails in the email server encrypted, emails can no longer be read by unauthorized entities, reducing unnecessary access to confidential information in emails.

As an IT administrator, can I enable employees to exchange files securely without impacting file size limits?

Yes. We made secure large file transfer easy to reduce the risk of employees using unapproved software to send large files. With the Entrust S/MIME solution, users can send protected files without the need for Zip files or passwords. Automated recipients' certificate selection and built-in file compression enable users to securely share large files and send to any number of internal or external recipients.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223

This is **Exhibit "B"** to the Affidavit of Dr. Gábor Lukács

affirmed before me on November 29, 2022

_____

Signature

SSL CERTIFICATE BASICS

CERTIFICATE SOLUTIONS FAQ

Site Seal

Site Seal

What is the Entrust Site Seal and why should I use it?

The best way to let your visitors know you have taken steps to ensure the security of their information is with the Entrust Secured Site Seal. Just by clicking the Entrust Secured Site Seal, visitors can verify your site's authenticity, and certificate status. Posting the Entrust Secure Site Seal on your website lets your website visitors know that you are committed to online security. Unless you deploy Extended Validation, the only indication of a secure connection customers get is a small lock on the bottom of

- Entrust receives notice or otherwise become aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of the CA's jurisdiction of operation.

What is Entrust's EV Certificate Problem Reporting and Response Capability?

Reporting
If you wish to revoke your Entrust Multi-Domain EV TLS/SSL Certificate for any of the above reasons, you may contact Entrust by filling in our online complaint form. In addition to Entrust Multi-Domain EV TLS/SSL Certificate revocation, Subscribers, Relying Parties, Application Software Vendors, and other third parties can contact Entrust by filling in our online complaint form for reporting complaints or suspected Private Key compromise, EV Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to EV Certificates.

Investigation

Entrust will begin investigation of all Certificate Problem Reports within twenty-four (24) hours and decide whether revocation or other appropriate action is warranted based on at least the following criteria:

- The nature of the alleged problem;
- Number of Certificate Problem Reports received about a particular EV Certificate or website;
- The identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered); and
- Relevant legislation in force.

Response

Entrust will maintain a continuous 24/7 ability to internally respond to any high priority Certificate Problem Report, and where appropriate, forward such complaints to law enforcement and/or revoke an Entrust Multi-Domain EV TLS/SSL Certificate that is the subject of such a complaint.

Secure Email Certificates

Do both parties need an Entrust Secure Email cert to communicate?

No, both parties just need an X.509 cert (public or private, any vendor)

Encryption — both parties should need an x.509 s/mime cert
Signing — only the signer needs a cert, the verifier doesn't

How do the parties exchange certificates if they are encrypting?

There is no central directory to publish the certs to, therefore the users who wish to encrypt need to exchange certs manually. This is commonly done by sending a signed email to the recipient, which "harvests" or collects the encryption cert

How does Entrust protect these private keys since they keep a backup of them for us?

The keys are stored in Entrust's secure facility, protected by a security level that no one customer would be able to provide on their own; it is the same protection offered by our public certificate business. They have the same level of protection as our CA keys, including aspects of physical security (room access), logical security (dual custody for access) and storage security (encrypted and integrity-protected with CA keys) This is not a case of any Entrust IT employee could get at these.

Does a re-issue of a certificate last for a year?

No, a re-issue has the same expiry as the original certificate, because it is at no charge. Only a renewal would offer a new term, and as a result would use another license/inventory.

Can I use the Secure Email certificates for MS Office Document signing?

Yes you can.

Does this ID offer non-repudiation?

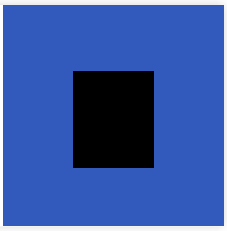
In order to offer the fully automated key backup, Entrust generates the private key on the Entrust server, and delivers it to the end-user in a P12 format. Because it is a dual-usage single key pair, the signing key is also generated on the Entrust server and not on the client machine. This may negate non-repudiation. We recommend you discuss this with your legal team.

Can I use my personal email account to obtain the certificate my corporation has purchased for me?

No. Because SMIME Enterprise certificates are Class II certificates, this means Entrust validates the organization and the email domain. The administrator approves or denies the certificate request. If your request does not match an email domain already verified by Entrust in your account, you will not be able to request the certificate. So since we cannot verify that “hotmail” or “gmail” are domains owned by your organization, you

cannot issue a SMIME Enterprise certificate to those types of email addresses. However, you would be able to issue the SMIME Personal certificate under a hotmail account, because we do not verify the email domain.

View FAQ



The Cloud

What is Entrust Certificate Services?

Entrust Certificate Services features a self-service tool that helps streamline the procurement and administration of TLS/SSL certificates. Acting as a centrally managed, self-service system, the service reduces administrative hassles and lessens the risk of inadvertent certificate expiration by issuing expiry notifications and allowing customers around-the-clock access to issue certificates. Entrust Certificate Services benefits include the following:

- Simplified enrollment
- Administrative management and delegation
- Client Management (for outsourcers, Web hosters, ISPs)
- On-demand services
- Cost savings
- Audit and reporting tools
- Zero footprint admin client
- Choice and flexibility of certificate types
- Strong verification process
- Additional information on Entrust Certificate Services can be found at: **https://www.entrust.com/digital-security/certificate-solutions/products/digital-certificates/tls-ssl-certificates/entrust-certificate-services**

How is the Entrust Certificate Service licensed?

The Entrust Certificate Service is available in two licensing options: Subscription and Units.

Subscription: Allows the management of a specific number of concurrent certificates over the term of the subscription. Subscription accounts allow the selection of specific certificate expiry dates and the re-use of certificate licenses to maximize usage. When