



## **OnlyKey WebCrypt and Virtru Hybrid Solution White Paper**

Prepared for Virtru Privacy Engineering Challenge

Prepared by: Tim Steiner

CISSP-ISSAP, OSCP, CEH, PMP

October 31, 2019

TABLE OF CONTENTS

**PROJECT BACKGROUND ..... 3**

**PROJECT OVERVIEW..... 4**

UNIVERSAL SUPPORT ..... 6

KEY MANAGEMENT ..... 6

USER SEARCH ..... 6

BETTER THAN OPENPGP ..... 7

BETTER THAN A SMART CARD..... 8

EASILY RECEIVE ENCRYPTED MESSAGES/FILES ..... 8

**A LAYERED SECURITY MODEL ..... 8**

**A ZERO TRUST SECURITY MODEL..... 9**

**INNOVATIONS, REACH, AND SOCIETAL IMPACT..... 9**

INNOVATIONS ..... 9

REACH..... 9

SOCIETAL IMPACT ..... 9

**ONLYKEY WEBCRYPT AND VIRTRU HYBRID WALKTHROUGH..... 10**

PROOF-OF-CONCEPT ..... 10

ENCRYPT ..... 10

DECRYPT ..... 11

**PRODUCTION** ..... 11

ENCRYPT ..... 11

DECRYPT ..... 12

**CONCLUSIONS..... 12**

# Project Background

---

CryptoTrust is a developer of secure solutions such as OnlyKey, and is continually developing innovative solutions to common security and privacy issues. OnlyKey was developed by a team of security experts and white hat hackers to stop malicious hackers. One thing hackers and malware on a computer cannot do is physically touch something.

- In order to use OnlyKey to authenticate, physical touch is required
- In order to read a secure message, physical touch is required
- In order to decrypt/sign files, physical touch is required

The reason for OnlyKey's design becomes clear when looking at the threat model of a typical computing environment.

As quoted by the CryptoTrust founder "As a security consultant and ethical hacker I would often be asked the question 'how do we securely manage passwords?' Before OnlyKey the best option was a software password manager. They are convenient, but software password managers can also be a huge security risk.

If your passwords are all stored on your internet connected computer or in the cloud then what happens if your computer gets malware or if the cloud is hacked? I regularly conduct tests for clients to identify security flaws and when I hear they use a software password manager I know that all I have to do is compromise one computer and then I will be able to access every account the user has. These accounts then provide access to additional resources and many times eventually lead to compromise of the entire enterprise."

Many times, it's not a matter of if a breach will occur but a matter of when. One click, or one malicious attachment in a phishing email opened by one user can result in an attacker accessing everything that user has access to and starting a chain of events that lead to complete compromise. Adding a physical hardware component has been found to neutralize employee phishing, Google has found that none of its 85,000+ employees were successfully phished since implementing hardware security devices that require physical touch<sup>1</sup>.

Not only does OnlyKey require physical touch, it requires a PIN entered on the device itself. This security feature gives OnlyKey an advantage over standard security keys (FIDO2 / U2F) and smart cards. If OnlyKey is lost it is unusable without the PIN and if a computer is compromised the PIN is not entered on a standard computer keyboard where it can be intercepted by malware. The OnlyKey PIN is entered on OnlyKey's six button keypad.

---

<sup>1</sup> <https://krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/>

**TRUST THAT YOU CAN TOUCH**  
One thing hackers and malware on a computer cannot do is physically touch something. Your direct physical approval is required to log in.

**EASY LOG IN**  
No need to remember multiple passwords because by plugging OnlyKey to your computer, it automatically inputs your username and password. It works with Windows, Mac OS, Linux, or Chromebook, just press a button to login securely!

**PROTECT ONLINE ACCOUNTS**  
A password manager, two-factor security key, and secure communication token in one, OnlyKey can keep your accounts safe even if your computer or a website is compromised. OnlyKey is open source, verified, and trustworthy.

**PIN PROTECTED**  
The PIN used to unlock OnlyKey is entered directly on it. This means that if this device is stolen, it becomes purposeless, after 10 failed attempts to unlock, data is securely erased.

**PORTABLE PROTECTION**  
Extremely durable, waterproof, and tamper resistant design allows you to take your OnlyKey with you everywhere.

ONLYKEY

## Project Overview

CryptoTrust recently released OnlyKey WebCrypt 2.0. This is an innovative web app that provides the ability to send and receive encrypted messages and files directly in popular web browsers without ever exposing secret/private keys to the browser.



### Securely encrypt and sign files using OnlyKey and Keybase PGP

Recipient's Keybase username or URL to their public PGP key or paste their key...

Enter a name to use for your encrypted files (optional)...

Choose the file(s) to encrypt

For best results total size of files should not exceed 70MB

No files selected.

Encrypt and Sign  Encrypt Only  Sign Only

## Security Goals of OnlyKey WebCrypt

**Make PGP easy:** Traditional PGP makes journalists angry, we think you shouldn't have to be technologically savvy to use PGP so we built WebCrypt.

**Empower the people:** Give people the ability to securely send and receive messages using any computer or Android device with no complicated software/drivers required and no worrying about compromise of user's private identity.

**Serverless:** All processing done via JavaScript in users own browser locally (no server to hack).

**Private:** No logins required. No data retention. No tracking!!! No emails. No ads. No demographics. Retain no metadata, or other tracking information.

**Strong crypto:** Everything should be sent via HTTPS to/from the web application. Data between local browser and OnlyKey should be encrypted using AES/ECDH shared secret (NaCl + AES-256-GCM). This means on the local computer data is end-to-end encrypted and even if a malicious applications were to intercept communication it would be encrypted and unreadable without the key.

**Phishing prevention:** All private keys are stored in secure hardware and all use requires user to authorize using physical touch on OnlyKey.

**Open source & audit-able:** What you see is what you get the OnlyKey WebCrypt repository is a Github page hosted directly on Github.

## Universal Support

This is accomplished by using the FIDO2 communication channel to communicate with a USB hardware device. The universal support for FIDO2 allows the web application to be used anywhere FIDO2 is supported including browsers Android, Windows, Mac OS, Linux, and Chromebook. The web app can also be released as a native app that does not require a web browser if this is preferred.

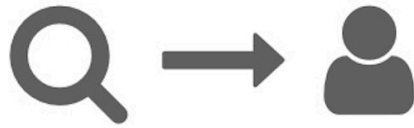
## Key Management

In addition to universal support, OnlyKey WebCrypt works with Keybase for easy user key management. Key management is one of the most difficult issues to solve when it comes to encrypting messages and files.


## User Search

The first step in secure communication is often finding the person to communicate with and having assurance that it is them. With the [OnlyKey WebCrypt Search](#) its easy to find users on Keybase by:

- Twitter, Github, Reddit, or Hackernews Usernames
- Web domains
- PGP fingerprint
- Or Automatically search for best match



Find Keybase user to send encrypted messages and files using OnlyKey and Keybase PGP

Auto search (searches any text for best match)  
Search For User  
Search results go here...  
Found a Match!  
  
Keybase Username = max  
Full Name = Max Krohn  
View this user's profile here  
Send this user encrypted message  
Send this user encrypted file  
Found a Match!  
Keybase Username = maxy  
Full Name = max

## Better than OpenPGP

OpenPGP is widely used but not exactly known for being easy to use. There have been efforts such as Keybase and Protonmail that make OpenPGP easier to use but require that private keys are accessible in software or the cloud.

This means that in some cases user's OpenPGP keys may be obtained by phishing attacks, malware, or software vulnerabilities. OnlyKey WebCrypt supports OpenPGP keys that are compatible with Protonmail, Keybase, Mailvelope, GPG, and others while allowing users to securely keep their keys offline.

## Better than a Smart Card

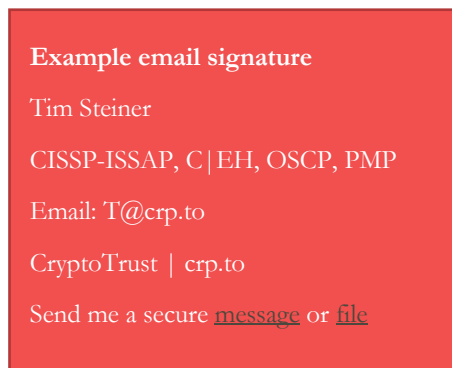
Smart cards are a popular way for keeping keys offline but they are not exactly known for being easy to use and are definitely not universally supported. OnlyKey provides similar function to a token/smart card but no drivers or software is required. Additionally, physical user presence is required to process secure messages/files. This is in contrast to Smart cards which only require a PIN code that can be captured and replayed without physical user presence allowing malware to decrypt a user's data.

## Easily Receive Encrypted Messages/Files

OnlyKey secure hardware is only needed for decryption of messages and files. Anyone can use the OnlyKey WebCrypt and Virtru hybrid solution to encrypt messages and files. For example, if a journalist wants to receive encrypted messages and files from a source, that source need only click a link to send the journalist a message that is encrypted via OpenPGP and encrypted again via Virtru. Unique links can be created for the journalist to place of a website or in an email signature as follows:

Send me a secure message - [https://apps.crp.to/encrypt.html?type=e&recipients=keybase\\_userid](https://apps.crp.to/encrypt.html?type=e&recipients=keybase_userid)

Send me a secure file - [https://apps.crp.to/encrypt-file.html?type=e&recipients=keybase\\_userid](https://apps.crp.to/encrypt-file.html?type=e&recipients=keybase_userid)



The issues solved by OnlyKey WebCrypt are issues that affect many at-risk communities such as human rights activists and journalists.

## A Layered Security Model

Layering multiple security solutions together for a high assurance security solution is not a new approach, but has received formal approval as being a model that is approved for securing even US government classified information with the Commercial Solutions for Classified (CSfC) program<sup>2</sup>. With the proposed OnlyKey WebCrypt and Virtru hybrid solution a similar high assurance model applies. As the data encrypted with the OnlyKey WebCrypt and Virtru hybrid solution a security issue with either solution alone does not result in compromise of the layered solution.

In addition to prevention of a single point of failure, the OnlyKey WebCrypt and Virtru hybrid solution permits clients to at the same time truly have a zero trust security model.

<sup>2</sup> <https://www.nsa.gov/Portals/70/documents/resources/everyone/csfc/csfc-customer-handbook.pdf>



# A Zero Trust Security Model

---

With either solution alone there is trust required. For Virtru a client is trusting Virtu's handling of private keys during key operations. Outsourcing key management may be an issue for some clients, such as those outside of the US or those with specific compliance requirements. For OnlyKey a client is trusting OnlyKey's handling and storage of private keys. Together the solutions form a zero trust security model as follows:

- First, OnlyKey WebCrypt encrypts data using OpenPGP.
- Second, the already encrypted data (Encrypted via RSA 2048/4096) is sent to Virtru for a second layer of encryption which may optionally add features like message expiration.
- Third, the client receives a TDF file that may only be decrypted if both authorized by Virtru and authorized by the physical OnlyKey device.

## Innovations, Reach, and Societal Impact

---

It becomes clear that with the proposed OnlyKey WebCrypt and Virtru hybrid solution there are many innovations, reach, and societal impacts.

### Innovations

- **Zero trust** - Many privacy focused individuals may not trust a centralized solution. The OnlyKey WebCrypt and Virtru hybrid solution provides zero trust and essentially a privacy guarantee. This novel layered approach is an advance in privacy engineering.
- **Defense in depth** – Each message/file is encrypted twice, by two different solutions ensuring there is no single point of failure. A vulnerability in OpenPGP will not affect the Virtru encryption and a vulnerability in Virtru implementation will not affect OpenPGP.
- **Universal support** – Privacy tools often go unused because of technical issues requiring the use of other methods (i.e. Mac computer does not have the right smart card drivers so a user sends unencrypted email). Universal support mitigates this by ensuring support for the most popular operating systems and browsers.
- **Time Limited Messages/Files** – Popular secure messenger solutions include features like disappearing messages. The addition of Virtru's message expiration enhances OnlyKey's message privacy enabling a feature that is a first of its kind, expiring OpenPGP or S/MIME encrypted messages.

### Reach

- **Increased Security and Compliance** - Hardware keys that require physical user presence have been shown to neutralize phishing attacks which are the number one way that attackers compromise organizations. Adding hardware key support for Virtru increases security of the overall solution and may help meet security policies and compliance mandates.
- **Increased Compatibility** - Hardware keys are not known for working out-of-the-box and often require complicated software installs. OnlyKey works out-of-the-box and directly in the browser on all popular desktop operating systems.

### Societal Impact

- The issues solved by OnlyKey WebCrypt are issues that affect many at-risk communities such as human rights activists and journalists.

- **Universal support** - Many journalists may travel and may have to make do with whatever internet connection that is available such as using a shared computer or a mobile device. OnlyKey WebCrypt does not require installing software, all that is needed is a USB port, a common web browser (i.e. Chrome, Firefox), and an internet connection.
- **Ease of Use** – It is often the case that secure solutions are not adopted not because of lack of availability but that they require considerable technical skills. For example, installing smart card software may require command line utilities and a high level of technical proficiency. At-risk communities may not have the technical proficiency to do this, with OnlyKey there are no commands necessary, setup is as easy as following step by step directions to generate a private key on Keybase and load onto the OnlyKey. This opens up the solution to a much wider range of at-risk communities.
- **Plausible Deniability** - Human rights activists and journalists may reside in or travel to countries with encryption bans or mandatory key disclosure. OnlyKey already has a feature for this to provide plausible deniability. Full details of this feature are available [here](#).

## OnlyKey WebCrypt and Virtru Hybrid Walkthrough

---

### Proof-of-concept

A proof of concept implementation is described below, this is publicly available for testing at <https://apps.crp.to/dev-vir/encrypt-file-vir-dev.html?type=e>

Note: The 'type=e' in the link tells the app to encrypt only, meaning on OnlyKey is not required (OnlyKey is only required for private key operations like signing)

### *Encrypt*

- 1) The sender browses to [OnlyKey WebCrypt](#), enters a Keybase user ID of the recipient, and selects “Set an expiration date/time.
- 2) The user is then prompted to perform 4 steps:
  - a) Step 1. Confirm your email below to enable expiration:
  - b) Step 2. Enter number of hours before file/message expires:
  - c) Step 3. Choose the file(s) to encrypt:
  - d) Step 4. Enter recipient’s email address:
- 3) Once the sender clicks encrypt the following occurs:
  - a) The public key is retrieved from Keybase
  - b) The file is zipped prior to encryption (speeds up encryption)
  - c) The file is encrypted via RSA 2048/4096 using the Keybase public key of the recipient (inner encryption)
  - d) The file is encrypted a second time using Virtru (outer encryption) and applies the expiration policy.
- 4) The encrypted TDF file is downloaded automatically to the user’s computer.

## *Decrypt*

- 1) The receiver browses to [OnlyKey WebCrypt](#) and adds a TDF file to decrypt, enters Keybase user ID of the sender and clicks “Decrypt.”
- 2) Once the sender clicks decrypt the following occurs:
  - a) The file is automatically detected as TDF type and the user is prompted to “Confirm your email below to decrypt TDF.”
  - b) The file is decrypted (outer encryption) by Virtru and if Virtru provides any errors such as the file is expired this message is displayed to user.
  - c) If Virtru decryption succeeds, the user is prompted to enter a 3 digit challenge code on their OnlyKey keypad, this unique code ensures that they are authorizing this decryption request.
  - d) If the correct challenge is entered, the file inner encryption is decrypted by OnlyKey.
- 3) The decrypted zip file is downloaded automatically to the user’s computer.

## **Production**

The proof-of-concept implementation has improvements and additional features that could be accomplished to create a better app. Those are shown in bold below:

## *Encrypt*

- 1) The sender browses to [OnlyKey WebCrypt](#) **(Or a private enterprise app)** enters **multiple recipient email addresses** or usernames, recipient may be autocompleted **(i.e. Office 365 Integration)**. Entering of the recipient would be similar to composing an email and **could be integrated with a mail client (i.e. Outlook)**. **The recipient could be automatically resolved** from Keybase ID to email address for Virtru recipient or vice versa, **instead of Keybase a private key server (GPG, S/MIME) could be used.**

**As production solution could be a web app, a native app, and/or an Outlook plugin. OpenPGP could be used or S/MIME for inner encryption.**

- 2) The user is then prompted to perform 3 steps:
  - a) Step 1. Confirm your email below to enable expiration (Virtru authentication session may already be established in which case this step would not be needed):
  - b) Step 2. Enter number of hours before file/message expires:
  - c) Step 3. Choose the file(s) to encrypt:
  - ~~d) Step 4. Enter recipient’s email address: (as mentioned, recipient could be automatically resolved from Keybase ID to email address for Virtru recipient or vice versa)~~
- 3) Once the sender clicks encrypt the following occurs:
  - a) The public key is retrieved from Keybase **(or the private key server)**
  - b) The file is zipped prior to encryption (speeds up encryption)
  - c) The file is encrypted via RSA 2048/4096 using the Keybase public key of the recipient (inner encryption)

- d) The file is encrypted a second time using Virtru (outer encryption) and applies the expiration policy.
- 4) The encrypted TDF file is downloaded automatically to the user's computer.

### *Decrypt*

- 1) The receiver browses to [OnlyKey WebCrypt](#) and adds a TDF file to decrypt **(Or opens file in private enterprise app)**, and confirms their email address with Virtru. **The TDF format could be used to inform the app that the message requires OnlyKey for inner encryption.**

**As noted above a production solution could just require email address for decryption.**

- 2) Once the sender clicks decrypt the following occurs:
- a) The file is automatically detected as TDF type and the user is prompted to confirm email to decrypt TDF (Virtru authentication session may already be established in which case this step would not be needed):
  - b) The file is decrypted (outer encryption) by Virtru and if Virtru provides any errors such as the file is expired this message is displayed to user.
  - c) If Virtru decryption succeeds, the user is prompted to enter a 3 digit challenge code on their OnlyKey keypad, this unique code ensures that they are authorizing this decryption request.
  - d) If the correct challenge is entered, the file inner encryption is decrypted by OnlyKey.
- 3) The decrypted zip file is downloaded automatically to the user's computer.

## Conclusions and Going Further

---

A hybrid of OnlyKey and Virtru would be a complementary solution that offers features and security benefits that each solution alone lack. Virtru does not have a physical security key that is required which may permit an attacker to compromise a Virtru user by compromise of the user's email account. OnlyKey does not have the advanced features that Virtru has such as expiring encrypted messages. Combined they would provide a full featured, high assurance encryption solution that would work virtually everywhere, and future features could be added offering even more benefits such as:

### **Expiration and Revocation for Any Type of Data (i.e. Authentication, FIDO2)**

It can be imagined that more than just messages and files can have expiration and revocation features, authentication credentials with these features would have many benefits. Imagine a software password manager that works in any browser (i.e. ITGlue) where each record is encrypted twice so that a security key and Virtru are required to access the record. OnlyKey is always ready to create new innovative features and technology to meet the security requirements of the future.