SECURITY TARGET
Virtru Data Protection Platform - Browser plug-in and Secure Reader - Version 7.14.1

Date : 19/12/2019

Version : 1. 4

Table of Contents:

Identification:

Document identification

This document is the Security Target (ST) of the product "Virtru Data Protection Platform - Browser plug-in and Secure Reader" developed by VIRTRU company. This ST is proposed to obtain the CSPN certification from ANSSI. The product is an email ciphering tool based on split knowledge mechanisms.

Product identification

Developer	VIRTRU
Developer website	www.virtru.com
Product commercial name	VIRTRU Data Protection Platform - Browser plug-in and Secure Reader
Version of the product	7.14.1
Product category	Messagerie sécurisée (Secure Messaging)

Product description

General description

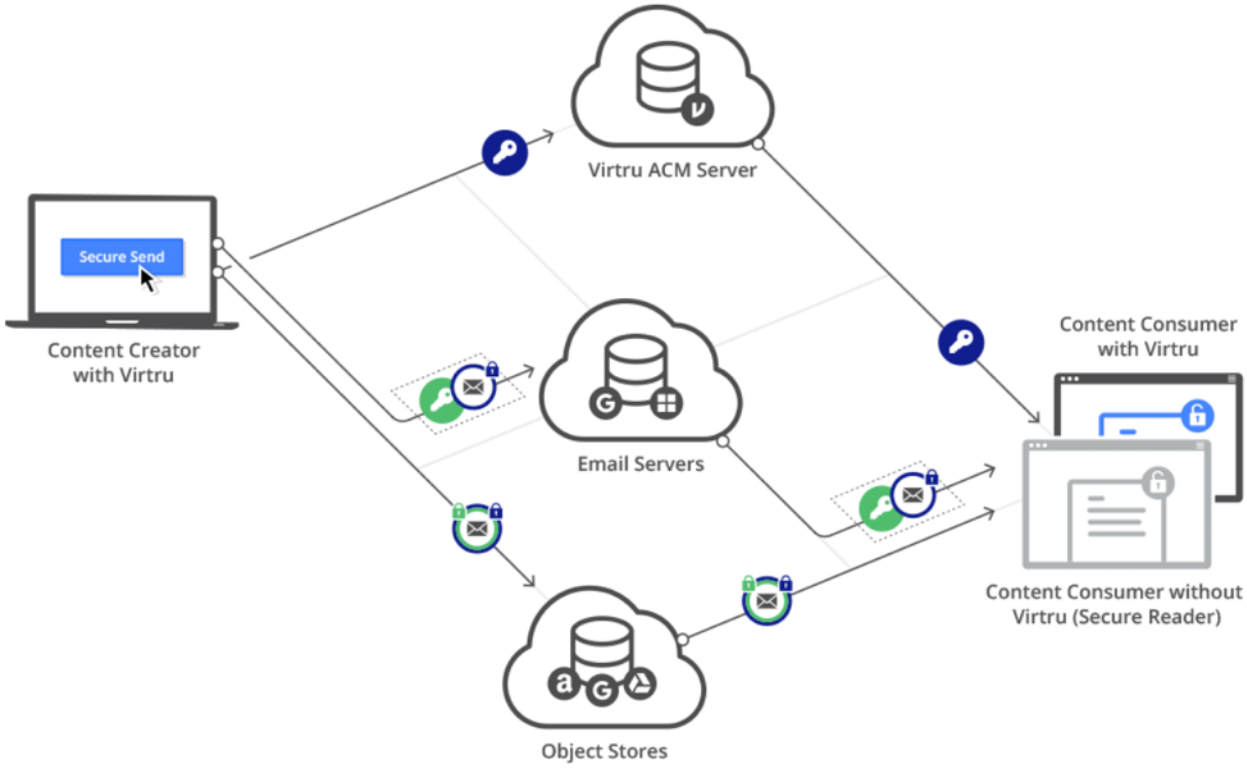
The Trusted Data Format (TDF) is an open standard for data centric security which allows granular data protection and access controls for any type of content. The TDF is designed for interoperability and works with any application, device, or platform. Developed by Virtru Chief Technology Officer and founder Will Ackerly, the TDF was originally designed for secure information sharing. The Virtru Data Protection Platform and all Virtru-enabled applications are built on the TDF standard.

Virtru is a data security company that protects corporate information from unauthorized access. Our patented Secure User-First Technology™ eliminates the tradeoff between data protection and ease of use by allowing users anywhere, on any device, to work the way they do today—without requiring a separate log-in, user interface or application.

Using the TDF, Virtru can encrypt and protect any data type and apply fine grained access control no matter how or where data is shared. Commonly deployed as part of a cloud migration, Virtru seamlessly integrates into platforms like Google G Suite and other Software-as-a-Service (SaaS) applications to make it easy to create and consume protected content. Virtru is Google's only recommended partner for encryption and data protection and was recently selected by Microsoft as one of only 11 companies for its prestigious Accelerator program for high growth partners. More than 5,000 organizations trust the Virtru Data Protection Platform to easily protect and control sensitive information regardless of where it's been created, stored or shared.

Virtru is offered as a SaaS platform for access control, policy enforcement, and key management. Data protection policies are enforced through integrations with Google G Suite and other SaaS business applications. Data protection policies are configured and enforced centrally, with optional client-side controls and notifications for end-users.

Features



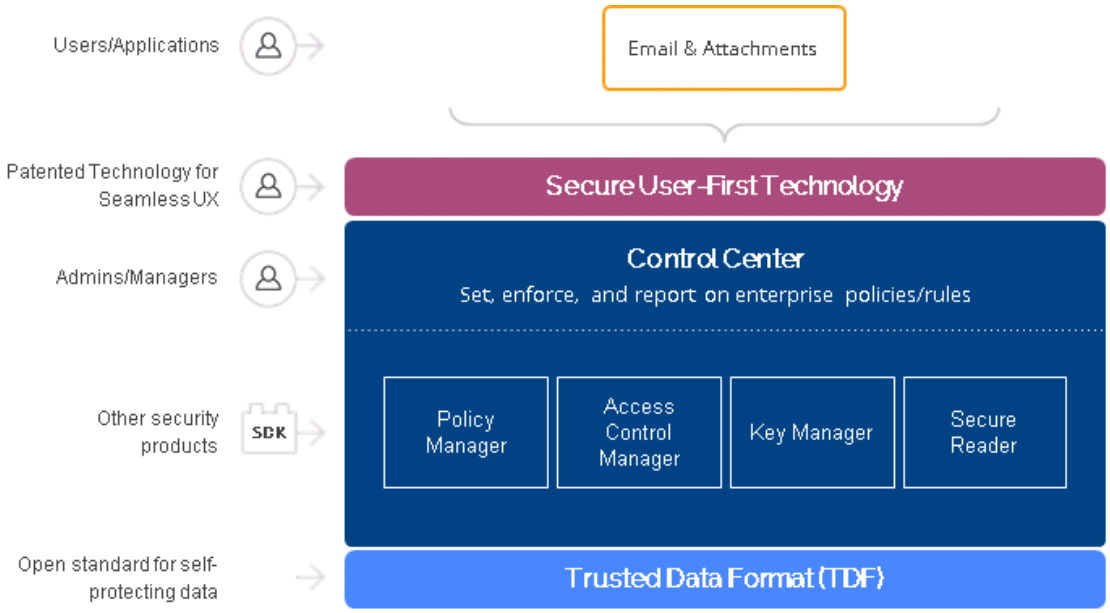
When using Virtru to secure emails, all messages and attachments are encrypted with AES 256-bit Galois/Counter Mode (GCM) Access Control Keys on the content creator's client via a browser extension, Microsoft Outlook plug-in, mobile app, or other Virtru-enabled client. Access control policies may also be applied at this time, either manually via the user or automatically via Data Loss Prevention (DLP) rules that are preconfigured by administrators. Examples of access control policies include: authorizing a party's access, setting expiration for this access, and enhancing content protection via PDF watermarking or download disablement.

Once email bodies are encrypted, they are sent via TLS 1.2 to the email server that will eventually deliver this content to authorized recipients. Cloud providers, such as Google and Microsoft, cannot access unencrypted content or decrypt content on their servers because they do not have access to the keys stored in the Virtru Access Control Manager (ACM). To allow recipients to read emails without installing Virtru's software, Virtru utilizes an external object store, Amazon S3, to surface encrypted emails via the Virtru Secure Reader application.

For each object, such as the individual email bodies and attachments, an individual Access Control Key is created and sent to the Virtru ACM. The content and key remain separate until a content consumer requests access to the encrypted email content. The sending Virtru client creates a copy of the email and any file attachments,

encrypts them with a separate key, known as the Payload Key, then encrypts the Payload Key with both the Access Control Key and an additional key, known as the Split Knowledge Key, and sends the encrypted content to the designated object store. The Split Knowledge Key is stored inside the email, which is delivered to the sender's specified recipients. Virtru services do not have access to the sender's or the recipient's email servers, ensuring that encrypted content stored in the external object store cannot be decrypted outside of an email recipient's Virtru client.

After authenticating, a content consumer with the Virtru client receives access to the Access Control Key (from the ACM) to decrypt the email content from their email server. A content consumer that does not have the Virtru client authenticates via the Secure Reader and uses the Split Knowledge Key (from their email server) and Access Control Key to decrypt the Payload Key, which decrypts the original email content.



Features offered by Virtru the technology include:

Dashboard: Provides dashboards for users and administrators to easily manage access to content and set centralized data protection policies. Allows administrators to configure client-side or network level rules for automatic protection and end-user warnings.

Access Control Manager (ACM): Allows content owners to assert, manage, and revoke who has access to sensitive material and for how long. Stores and enables access to encryption and decryption keys by authorized users.

Secure Reader: Authenticates and verifies content consumers using either federated identity services (e.g.: OAuth) or email confirmations. Enables client-side decryption of messages for recipients who do not have a Virtru plug-in installed.

Domain Worker: Imports customer organization's identification information (emails, names, group memberships) for a customer domain.

Audit Worker: this service allows recording of events associated with messages life-cycle (send, read, etc.) or data protection policies (revocation, expiration, etc.)

Virtru Client/Plug-in: (installed on the client browser or mail software) offers the following features:

- Enables client-side protection at the time of creation.
- Communicate with the Virtru ACM for access control, key management, and policy enforcement.
- Enable decryption when the application receives protected content and the content consumer is authorized.

ToE perimeter

The evaluation is focused on the sender and the recipient part of the Virtru Platform:

- Virtru-plug in
- Virtru Secure reader

For the purpose of this evaluation, the following features will be in the perimeter of the evaluation:

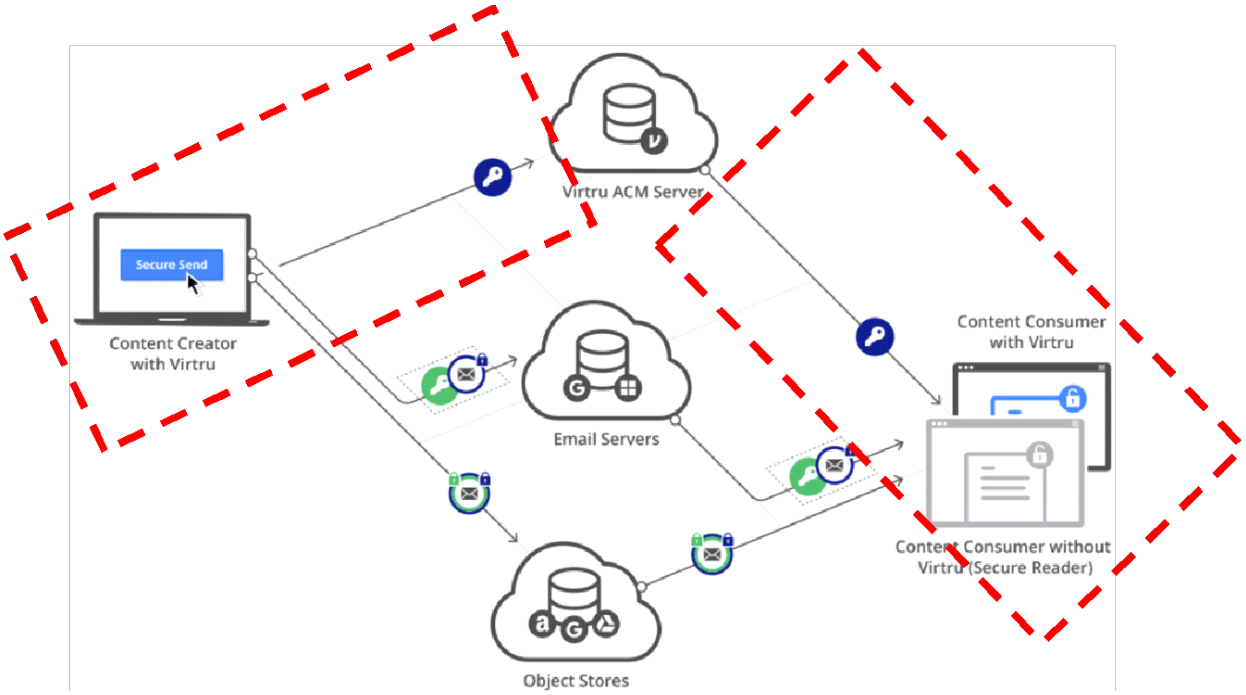
- All features of the Virtru client plug-in (client-side encryption, communication with Virtru services, and decryption of the protected content)
- All features of the Virtru Secure Reader (client-side encryption, communication with Virtru services, and decryption of the protected content)

All services between the sender and the recipient are not under evaluation and should be considered as potentially hostile (Amazon S3 used to store objects, Virtru ACM server on Amazon EC2)[1].

The general goal of this evaluation is to ensure that:

- only the sender and the recipient of the messages are able to decrypt the content of the messages
- Virtru clients encrypt data in such a way that third-parties cannot decrypt the data
- Virtru plug-in doesn't introduce vulnerabilities in the client mail software or operating system.
- the split knowledge technology developed by Virtru allows end-users to protect their messages without relying on the security of third parties

[1] See Attackers profiles in the chapter « Threat Model »



ToE Perimeter (red dotted line)

Product usage

Virtru can be used in two ways:

- Both the sender and recipient of messages are enrolled Virtru users.
- The sender is an enrolled Virtru user, but the recipient of the message is not.

Sender and recipient when enrolled in Virtru platform can use Virtru plug-ins to embed the Virtru features in their mail client software like Google Mail (Gmail)..

The users that may interact with the ToE are the following:

- Sender of the message (enrolled on Virtru platform).
- Recipient of the message (enrolled or not in Virtru platform).

Users are authenticated to the Virtru client or Secure Reader by OAuth from their identify provider or by email confirmation (Secure Reader only). The user enables Virtru protection with the Virtru client. Replies from the Secure Reader are automatically protected by Virtru.

Operating environment

The intended operating environment for Virtru is composed of:

- Virtru Browser Plug-in installed on Google Chrome using Gmail
- Secure Reader in a web browser
- Operating systems for workstation: Windows, MacOS, Linux
- Operating system for ACM Server: Ubuntu 16.04 on AWS EC2
- Databases: AWS DynamoDB and S3

For the purpose of the evaluation, the tested platform will be:

- Plug-in: Browser Plug-in Version 7.14.1 using Gmail
- Workstation Operating system: Windows 10
- Chrome version: 79.0.3945

Security perimeter

Users

The users that may interact with the ToE are the following:

- Sender of the message (enrolled on Virtru platform).
- Recipient of the message (enrolled or not in Virtru platform).

Users are individuals that need to exchange in a sensitive data with contacts that can be enrolled or not on the Virtru platform.

Assumptions

A.SAFE_WORKSTATION	It is assumed that the workstations where email are sent or received (through the Virtru plug-in or using Secure reader) are secure and free from viruses or malware.
A.USERS_NOT_EVIL	ToE users are trained for performing the tasks they are responsible for. They follow instructions and user manuals of the ToE and they are not hostile.
A.SAFE_AUTHENTICATION	It is assumed that the Identity provider or the authentication performed by email confirmation are secure and safe. Email confirmation is assumed to be delivered to the right recipient.

A.SAFE_SMTP_RELAY	It is assumed that emails exchanged between the senders and the recipients are correctly relayed.
A.SECURE_MAILBOX	Attacks against the user mailbox itself are not considered (malicious SMTP server administrator or mailbox takeover by an attacker).

Critical Assets

CA.ACCESS_CTL_KEY	Access Control Key used to encrypt messages. Each message has its own Access Control Key. The key is generated on the sender workstation.
CA.KEYMGR_TLS_KEY	The key used for TLS communications with Key Manager on Virtru Services server (communication from the client).
CA.SPLIT_KEY	Split Knowledge Key is used to encrypt the Payload Key. The Split Knowledge Key is sent in clear-text with the message.
CA.PAYLOAD_KEY	Payload Key used to encrypt a copy of the plaintext message or attachment for storage in AWS. The Payload Key is encrypted by the Split Knowledge Key and Access Control Key.
CA.MESSAGE[2]	Message that is sent from a Virtru registered client to a recipient.

Security needs for critical assets are summarized in the following table:

Critical Asset	Availability	Confidentiality	Integrity	Authenticity
CA.ACCESS_CTL_KEY		●	●	●
CA.KEYMGR_TLS_KEY		●		●

[2] It should be noted that the original message of the user always contains additional information specific to Virtru in order to allow the deciphering for non-Virtru users;

CA.SPLIT_KEY		●[3]	●	●
CA.MESSAGE		●	●	●
CA.PAYLOAD_Key		●	●	●

Threat model

Attackers

Attackers that are considered for this evaluation are the following:

- Attacker having access to the network between the sender and the recipient of the message allowing him/her to intercept communications.
- Attacker having access to services between the sender and the recipient (Amazon S3 used to store objects, Virtru ACM server, ACM DynamoDB table). Such attacker could have access to several keys included in the ciphering process, but not all at the same time (Access Control Key for someone having access to Virtru ACM Server, Split Knowledge Key for someone having access to SMTP server, Payload Key for someone having access to Amazon S3).

Threats

M.ACK_KEY_INTERCEPT — An attacker intercepts an Access Control Key during its transmission to the Virtru Server allowing him/her to try to decipher messages retrieved using the threat M.MESSAGE_INTERCEPT.

M.MESSAGE_INTERCEPT — An attacker intercepts a message, which contains the Split Knowledge Key, during its transmission to the recipient.

[3] It is the combination of Split Knowledge Key and Access Control Key that need confidentiality.

Security functions

F.ENCRYPT_MESSAGES

The ToE encrypts messages and attachments on the sender's client (Browser Plugin or Secure Reader in Google Chrome Browser) using a specific access control key (CA.ACCESS_CTL_KEY) for each message. The ciphering is performed using AES256 GCM algorithm. The encrypted message is sent to the recipient of the email using regular SMTP messaging system while the access control key is transferred to the Virtru ACM server using the ToE security function F.PROTECT_FLOW_Key (see below).

In order to support decryption for users without the Virtru plugin installed by using the Secure Reader and for attachments, the ToE additionally re-ciphers the message previously ciphered by the Access Control Key using a specific payload key (CA.PAYLOAD_KEY)[4]. This key is first encrypted with the Access Control Key (CA.ACCESS_CTL_Key) and then ciphered using a Split Knowledge Key (CA.SPLIT_KEY). The Split Knowledge Key is transmitted in clear-text in the email while the message ciphered by the Payload Key and Access Control Key is stored in AWS. Payload Key is also stored in AWS protected by the Split Knowledge Key.

F.DECRYPT_MESSAGES_VIRTRU_USER

The recipient of a message who is registered and uses the Virtru plug-in receives the encrypted message. Then the ToE retrieves the Access Control Key (CA.ACCESS_CTL_Key) associated with the message from the Virtru ACM, by checking that all policy requirements (authorized user, expiration date, etc.), and deciphers the message (CA.MESSAGE) from the email server on the client. If there are any attachments in the encrypted message, they are decrypted following the process described below in (F.DECRYPT_MESSAGES_NON_VIRTRU_USER)

F.DECRYPT_MESSAGES_NON_VIRTRU_USER

When the recipient of the message is not a Virtru user, the Secure Reader is used to decrypt the message. The recipient connects to the Secure Reader from their web browser and authenticates themselves using a third party identity provider or by email confirmation. When recipient is authenticated, he/she retrieves the Access Control Key from ACM server while the ciphered Message and the ciphered Payload Key are retrieved from AWS. Cookies used for authentication to the Virtru ACM are

[4] The message is multi-ciphered

valid for 120 days, unless expired through explicit user logout or extended open session on the screen. Now the recipient can:

- Decipher the Payload Key using the Access Control Key and Split Knowledge Key.
- Decipher the message using the Payload Key.

F.PROTECT_FLOW_KEY

The ToE protects the communication of the Access Control Key from the sender workstation to the ACM Virtru Server or from recipient workstation to the ACM Virtru Server using a TLS communication.

Threats are covered by the security functions as shown in the following table :

SECURITY FUNCTION / THREATS	M.ACK_KEY_INTERCEPT	M.MESSAGE_INTERCEPT
F.ENCRYPT_MESSAGES		●
F.PROTECT_FLOW_KEY	●	
F.DECRYPT_MESSAGES_VIRTRU_USER		●
F.DECRYPT_MESSAGES_NON_VIRTRU_USER		●

Mapping

ASSETS / THREATS	M.ACK_KEY_INTERCEPT	M.MESSAGE_INTERCEPT
CA.ACCESS_CTL_KEY	●	

CA.KEYMGR_TLS_KEY		●
CA.SPLIT_KEY		●
CA.MESSAGE		●