31 DEC 2024

Document Version 1.2

VIDCALL VERSION 8.2

SECURITY TARGET

vidcall

For more information visit us at

www.biocryptodisk.com

Document management

Document identification

Document Title	Vidcall Version 8.2 Security Target
Document Version	1.2
Document Date	31-DEC-2024
Release Authority	Advanced Product Design Sdn Bhd

Document history

Version	Date	Description
0.1	25-OCT-2023	Initial Released
0.2	09-NOV-2023	Update Section 1 and Section 6
0.3	22-DEC-2023	Update Section 1, Section 5 and Section 6 based on evaluator’s comment
0.4	12-FEB-2024	Update Section 1, Section 3, Section 4, Section 5 and Section 6 based on evaluator’s comments in MySEF-3-EXE-E052-EOR1-d1
0.5	16-FEB-2024	Update Section 1, Section 5 and Section 6
0.6	26-FEB-2024	Update Section 1, Section 5 and Section 6 based on evaluator’s comments in MySEF-3-EXE-E052-EOR1-d2
0.7	04-MAR-2024	Update Section 1 and Section 6
0.8	02-MAY-2024	Update Section 1 until Section 6 based on evaluator’s comments in MySEF-3-EXE-E052-EOR2 until EOR4
0.9	28-MAY-2024	Update Section 1 until Section 6 based on evaluator’s comments in MySEF-3-EXE-E052-EOR2-d3 and MySEF-3-EXE-E052-EOR4-d2
1.0	24-JUNE-2024	Update Section 4 based on evaluator’s comments in MySEF-3-EXE-E052-EOR4-d3
1.1	18-JULY-2024	Update Section 6.3
1.2	31-DEC-2024	Update the Front Page, Section 1, Section 4 and Section 6 based on evaluator’s comments Final Released

Table of Contents

1 Security Target Introduction (ASE_INT.1)

1.1 ST Reference

ST Title	Vidcall Version 8.2 Security Target
ST Version	1.2
ST Date	31-DEC-2024

1.2 TOE Reference

TOE Title	Vidcall
TOE Version	Version 8.2

1.3 Document Organization

This document is organized into the following major sections:

- Section 1 provides the introductory material for the ST as well as the TOE description (ASE_INT.1).

- Section 2 provides the conformance claims for the evaluation (ASE_CCL.1).

- Section 3 provides the definition of the security problem that the TOE has been designed to address (ASE_SPD.1).

- Section 4 defines the security objectives for the TOE and the environment (ASE_OBJ.2).

- Section 5 contains the security functional and assurance requirements derived from the Common Criteria, Part 2 and 3 respectively, which are in turn satisfied by the TOE and the development lifecycle (ASE_REQ.2).

- Section 6 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE (ASE_TSS.1).

1.4 Defined Terms

The following table defines all subjects, objects, operations, security attributes, external entities and other key terms that are used within the statements of security functional and assurance requirements. It also describes the acronym used in this documentation.

Table 1 - Defined Terms

Term	Description
AES	Advanced Encryption Standard (AES) is a symmetric-key encryption defined in Federal Information Processing Standard (FIPS) Publication 197. The standard comprises three block ciphers, AES-128, AES-192 and AES-256.
AES CBC Mode	The CBC-AES algorithm is a mode of operation of the Advanced Encryption Standard (AES) algorithm. (The acronym CBC stands for Cipher Block Chaining)
AES-256-CM-HMAC-SHA1-80	AES-CM-256: This indicates the use of the Advanced Encryption Standard (AES) with a 256-bit key size in Counter Mode (CM). AES is a widely used symmetric encryption algorithm, and the key size (256 bits in this case) determines the strength of the encryption. Counter Mode (CM) is a mode of operation for block ciphers like AES This part specifies the use of Hash-based Message Authentication Code (HMAC) with the SHA-1 hash function, truncated to 80 bits. HMAC is a method of ensuring the integrity and authenticity of a message using a cryptographic hash function.
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
OAuth 2.0	OAuth 2.0 is an open standard for authentication and authorization. It provides a framework for secure access to resources without exposing the user's credentials to the client application.
RAM	Random Access Memory
Remote Users	TOE users that interact indirectly with the TOE through another IT product. Example: For TOE user to interact with the TOE web application, TOE user has to use TOE user's workstation and web browser For TOE user to interact with the TOE software, TOE user has to use TOE user's workstation

Term	Description
SIP	Session Initiation Protocol
SRTP	SRTP also known as Secure Real - Time Transport Protocol, is an extension profile of RTP (Real-Time Transport Protocol) which adds further security features, such as message authentication, confidentiality and replay protection mostly intended for Audio and Video communications.
Authorised User	Authorised user is an admin user who manages the system management console. Note that Authorised user and system management console are out of the scope of evaluation
TOE	Target of Evaluation
TOE Users	Users that able to login to the TOE and access the TOE features stated in Section 1.5.1 and Section 1.6.1
TSF	TOE Security Function
User data	Data created by and for the user, which does not affect the operation of the TSF.

1.5 TOE Overview

1.5.1 TOE Usage and Major Security Functions

The TOE is Vidcall Version 8.2. The TOE is a web and software application designed to facilitate virtual meetings, conferences, chat and messaging and collaborations while prioritizing the protection of sensitive information and the privacy of participants. The TOE enables individuals or groups to connect and interact in real-time, regardless of their physical locations.

The TOE typically offers a range of features to make virtual meetings, chat and messaging more effective and efficient, including:

- Video Conferencing: TOE users can see and interact with each other through live video feeds, creating a more engaging and personal meeting experience. The video conferencing is end to end encrypted between host and client

- Audio Conferencing: TOE users can communicate via voice, which is essential for meetings with poor internet connections or when video is not required.

- Audio/Video peer to peer call. The audio and video traverse end to end encrypted between two TOE users without involving media server

- Screen Sharing: This feature allows TOE Users to share their screens, making it easy to present documents, slideshows, or software applications.

- Chat and Messaging: Text-based chat and messaging features facilitate real-time communication and sharing of links, files, or messages during the meeting.

- Meeting Recording: Recording of meetings

- Watermark: Watermark of user screen so to discourage meeting clients to do recording without meeting host knowledge.

- File Sharing: The TOE includes the capability to share files and documents directly within the meeting.

- History: The TOE generates audit records for security events such as TOE users login and logout activities, reset password and reset password request. TOE users have the ability to view the audit logs.

The TOE is designed with robust security features to safeguard sensitive information, maintain privacy, and prevent unauthorized access or data breaches during online interactions. The following table highlights the range of security features implemented by the TOE:

Table 2 - Security Features

Security Features	Descriptions
Security Audit	The TOE generates audit records for security events such as TOE users login and logout activities, reset password and reset password request. TOE users have the ability to view the audit logs.
Cryptographic Support	The TOE implements encryption algorithms that utilize ECC (Prime256v1), AES256 CBC Mode, ECIES (Prime256v1), ECDSA (Prime256v1) and AES-256-CM-HMAC-SHA1-80
Identification and Authentication	TOE users are required to identify and authenticate before they are able to perform the TOE operations stated in Section 6.4.
Secure Communication	The TOE can protect the user data from disclosure and modification by using TLS v1.2, OAuth 2.0 Bearer Tokens (RESTful APIs) and SRTP (AES-256-CM-HMAC-SHA1-80) as a secure communication

1.5.2 TOE Type

The TOE is a virtual meetings, conferences, chat and messaging and collaborations web and software application that provides features such as video conferencing, audio conferencing, Audio/Video peer to peer call, screen sharing, chat and messaging, meeting recording, watermark, file sharing and history. The TOE provides security functionality such as Security Audit, Cryptographic Support, Identification and Authentication and Secure Communication. The TOE can be categorised as *Other Devices and Systems* in accordance with the categories identified in the Common Criteria Portal (www.commoncriteriaportal.org).

1.5.3 Non-TOE hardware/software/firmware

The underlying hardware and software that is used to support the TOE are:

Table 3 - Minimum System Requirements

Minimum System Requirements	
Web Server (TOE Web Application)	
Processor	Intel Xeon E-2224 Quad-core processor Clock Speed: 3.4 GHz
Operating System	Windows Server 2019 Standard Edition (64-bit)
Memory (RAM)	32GB RAM
Storage	2TB
TOE Users Workstation (TOE Software Application)	
Processor	2.4GHz Intel Core 2 Duo PC with Intel or AMD processors
Operating System	Windows 10

Memory (RAM)	8GB RAM
Storage	500 GB
Web Browser	Microsoft Edge 123 Mozilla Firefox 125 Google Chrome 124

The TOE user who wants to host the meeting shall use a PC with an Intel GPU and be connected to the internet using an Ethernet cable. In this configuration, video conferencing is end to end encrypted.

1.6 TOE Description

1.6.1 Physical Scope of the TOE

A typical implementation of the TOE can be found in Figure 1 below, which identifies the various components of the TOE architecture.

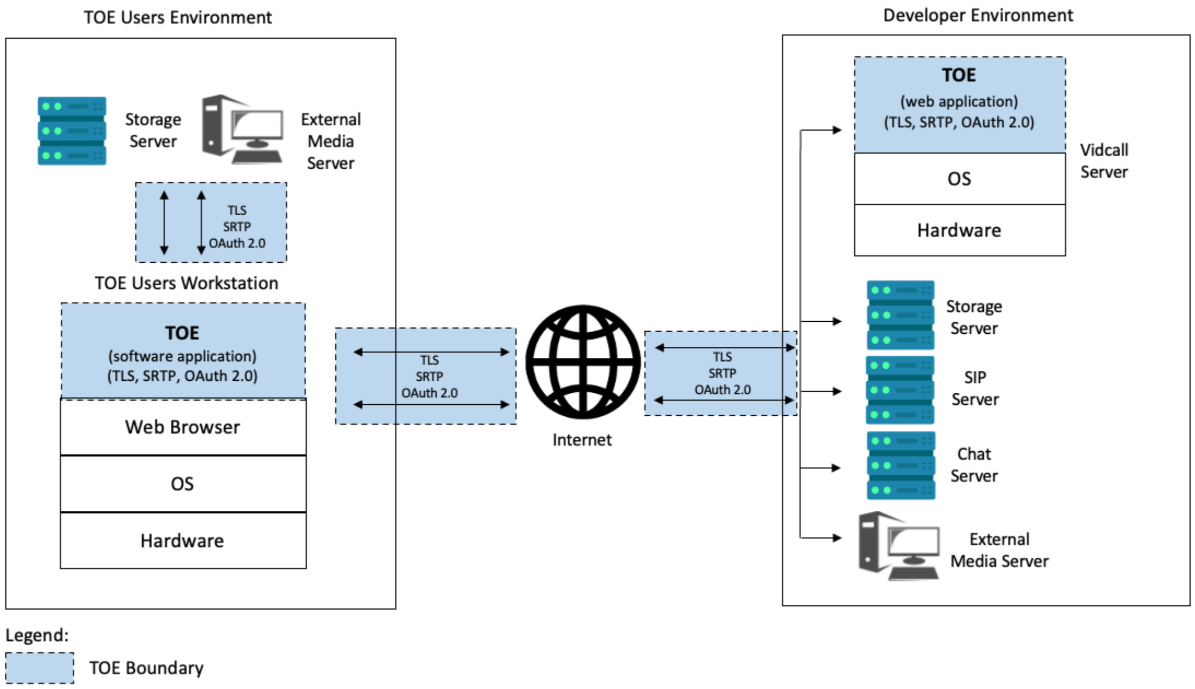

Figure 1 - TOE Physical Scope

The TOE consists of two parts; TOE web application and TOE software application. The TOE web application is used by the TOE users to perform TOE users registration, change TOE users password, enable two-factor (2FA) authentication. The TOE user accessed the TOE web application via a supported web browser stated in Section 1.5.3 (installed on the TOE users workstation)

The TOE software application (installed on the TOE users workstation) is used to perform TOE operation such as video conferencing, audio conferencing, audio/video peer to peer call, screen sharing, chat and messaging, meeting recording, watermark, file sharing and history.

Below is the TOE user registration process flow:

- User Registration: The TOE software application will be downloaded and installed by the TOE user. The TOE software application can be downloaded by the TOE user by visiting to https://1dataonline.com/home/homepage. On the homepage, simply click the "Download" button to download the installer necessary for installation. For new registration, TOE users need to browse to the TOE web application (https://1dataonline.com/authentication/Register) to register for a new account. They have to fill out all the required information such as Email, Display Name, Password and Retype Password and then click 'SIGN ME UP' to register. Upon registration, TOE users will receive a verification email in TOE user's email inbox.

- User login: After the registration and email validation, the TOE users have to wait till the authorised user activation before they are able to login via the TOE software application (vidcall_8.2.exe (Windows)) and TOE web application (https://1dataonline.com/authentication/Login)

In order to perform the TOE operation, the TOE will need to communicate with several servers that are hosted locally in the developer environment which is located in Malaysia. There are five (5) servers involved:

- Vidcall Server: Web Server is a server to host the TOE web application and system management console. System management console is a web based system used by the authorised user to manage the TOE users. Note that the system management console is out of the scope of evaluation.

- External Media Server: The Media Server is a PC that utilizes an Intel GPU and is connected to the internet via an Ethernet cable, which is also known as Ethernet Intel. The PC used for standby media server purposes is out of the scope of testing. This ready media server will act as a host if the TOE user who wants to host the meeting does not meet the media server requirement

- SIP Server: A SIP server or SIP proxy processes session initiation protocol (SIP) requests. This server is the main element of an IP private branch exchange. SIP is an internet protocol used to initiate and receive voice and video communication by transmitting data packets across an internet connection. This enables the quick and easy transmission of SIP calling between 2 or more parties.

- Chat Server: A Chat server is a central application or system in a client-server architecture that manages and maintains real-time communication among multiple users connected over the internet. It facilitates message exchange and ensures that the chat data is delivered correctly to the intended recipients. Chat messages are end to end encrypted and each message is digitally signed.

- Storage Server: The storage server is used to temporary store the files attached in the TOE (software application). When a user send an attachment to another user, the TOE (software application) will upload the encrypted file to the storage server. The recipient will then download the encrypted file from the storage server. Data stored is encrypted for both chat messages and attachment and can only be accessed via successful log in to TOE (software application). As stated above, storage server is a temporary storage location for file attachment during chat and messaging and video conferencing. A storage server can be located inside or outside of developer environment or at TOE user designated location.

Note that these five (5) servers are out of the scope of evaluation.

If any issues occur, the TOE users can communicate via a phone call, email or meet face-to-face with the developer to resolve the issue via contact information provided below:

- Advanced Product Design Sdn Bhd (Developer)

  No 209, Jalan Impian Emas 22, Taman Impian Emas, 81300 Skudai, Johor, Malaysia.

  Website: www.biocryptodisk.com

  Email: marketing@biocryptodisk.com

  Phone No: +607-550 4855 / +6012-7769949

The TOE includes the following guidance documentation; Vidcall User Manual Media Server 0.97.pdf, Vidcall User Manual Windows 1.2.pdf, Vidcall Web Application User Manual 0.96.pdf

1.6.2 Logical Scope of the TOE

The logical boundary of the TOE is summarized below:

- **Security Audit.** The TOE generates audit records for security events. The type of audit logs are user login and logout activities, reset password and reset password request. TOE users have the capability to view these audit logs via the TOE Software.

- **Cryptographic Support.** The TOE implements encryption algorithm that utilizes:
  - ECC (Prime256v1)

  - ECIES (Prime256v1)
  - ECDSA (Prime256v1)
  - AES256 CBC Mode
  - AES-256-CM-HMAC-SHA1-80

- **Identification & Authentication.** TOE users are required to be identified and authenticated before they are able to perform TOE operations stated in Section 6.4. At the login page (for both TOE web and software application), TOE users need to key in a valid username and password in order to access the TOE. The acceptable password should at least 8 characters in length and should include at least 1 uppercase letter, 1 number, and 1 special characters. TOE users have the option to enable the two-factor authentication (2FA). 2FA can be enabled by login to the TOE web application.

- **Secure Communication.** The TOE can protect the user data from disclosure and modification by utilizing HTTPS (TLS v1.2), OAuth 2.0 Bearer Tokens and SRTP (AES-256-CM-HMAC-SHA1-80)

2 Conformance Claim (ASE_CCL.1)

This ST and the TOE it describes are conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017
    - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017
    - Part 3 Conformant

This ST and the TOE it describes are conformant to the following package:

- EAL2

3 Security problem definition (ASE_SPD.1)

3.1 Overview

This section describes the nature of the security problem that the TOE is designed to address. The security problem is described through:

a) a series of ***threats*** that the TOE has been designed to mitigate,

b) specific ***assumptions*** about the security aspects of the environment (both IT related and non-IT related elements) in which the TOE will operate, and

c) any relevant ***organisational security policies*** are any statements made in terms of rules or guidelines that must be followed by the TOE and/or the operational environment.

3.2 Threats

Identifier	Threat statement
T.COMINT	An unauthorised user may attempt to compromise the integrity of the data collected, processed and transmitted by the TOE by bypassing a security mechanism.
T.DISCLOSURE	An unauthorised user may attempt to compromise the integrity of the protected resource on the TOE
T.IMPERSON	An attacker may gain unauthorised access to information or resources by impersonating an authorised user of the TOE.
T.PASSWORD	An unauthorized user may take advantage of weak administrative passwords to gain privileged access to the TOE functions.

3.3 Organisational security policies

No organisational security policies have been defined regarding the use of the TOE.

3.4 Assumptions

Identifiers	Assumption statements
A.AUTHORISE	The TOE user is not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the developer

Identifiers	Assumption statements
A.OPSYS	The operating systems supporting the TOE components protect against the unauthorised access, modification or deletion of the individual TOE components that they host.
A.UPDATE	The underlying platform on which the TOE operates will be regularly updated with the latest security patches and fixes to ensure data stored on the platform remains protected and secure.
A.FIREWALL	The IT environment will implement gateway filtering; only allowing HTTP and HTTPS inbound connection traffic to pass through to TOE.
A.OS	The authorised user shall ensure the OS backend server have been hardened to counter the perceived threats.
A.TIMESTAMP	The platforms on which the TOE operate shall be able to provide reliable time stamps.

4 Security objectives (ASE_OBJ.2)

4.1 Overview

The security objectives are a concise statement of the intended response to the security problem defined in Section 3. There are security objectives for the TOE to address and additional objectives that provide specific direction for the intended in environment in which the TOE is to operate.

4.2 Security objectives for the TOE

Identifier	Objective statements
O.AUTHENTICATE	The TOE must ensure that all TOE users are authenticated before they access a protected resource or functions.
O.KEYPROTECT	The TOE must ensure that all cryptographic keys stored within the TOE are protect sufficiently to prevent their disclosure to a malicious entity.
O.CRYPT	The TOE implements cryptographic functions compliant to the relevant industry standards.
O.TOECOM	The TOE must protect the confidentiality of its dialogue between distributed components from disclosure and modification
O.PASSWORD	The TOE must ensure that the TOE user password has a minimum of 8 characters in length, at least 1 uppercase letter, 1 number, and 1 special characters
O.LOGGING	The TOE shall log security-relevant actions and allow only TOE User to view them

4.3 Security objectives for the environment

Identifier	Objective statements
OE.INSTALL	The TOE shall be downloaded and installed by the TOE users in accordance to the guidance document provided by the developer
OE.AUTHORISE	The TOE user assigned to operate the TOE is trusted by the organisation and are trained in use of the TOE.
OE.OPSYS	The operating system on the underlying platform shall meet the minimum requirements for the TOE and shall be updated prior to installation to provide underlying security to the TOE.
OE.UPDATE	The developer shall provide updates of the TOE on a regular basis.

OE.FIREWALL	The IT environment will implement gateway filtering; only allowing HTTP and HTTPS inbound connection traffic to pass through to Web server. The Web server would only accept service requests from the corresponding service provider. The TOE web and software application only accepts service requests from authorised service applications
OE.OS	The operating systems selected are of sufficient hardness to counter the perceived threats. The server-side hardness includes capabilities to establish a secure configuration to the OS, configure OS audit logs, configure proper OS authentication and permission, and ensure legacy services are not enabled.
OE.TIMESTAMP	Reliable timestamp is provided by the operational environment for the TOE.

4.4 TOE security objectives rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions and threats.

Table 4 - TOE Security Objectives Rationale

Threats/ Assumptions Objectives	T.COMINT	T.DISCLOSURE	T.IMPERSON	T.PASSWORD	A. AUTHORISE	A.OPSYS	A.UPDATE	A.FIREWALL	A.OS	A.TIMESTAMP
O.AUTHENTICATE		✓	✓							
O.KEYPROTECT		✓								
O.CRYPT	✓	✓								
O.TOECOM	✓									
O.PASSWORD				✓						
O.LOGGING			✓							
OE.INSTALL							✓		✓	
OE.AUTHORISE					✓					
OE.OPSYS						✓	✓		✓	

Threats/ Assumptions Objectives	T.COMINT	T.DISCLOSURE	T.IMPERSON	T.PASSWORD	A. AUTHORISE	A.OPSYS	A.UPDATE	A.FIREWALL	A.OS	A.TIMESTAMP
OE.UPDATE							✓		✓	
OE.FIREWALL								✓		
OE.OS						✓	✓		✓	
OE.TIMESTAMP										✓

4.4.1 Rationale for security objectives of the TOE

The following table demonstrates that all security objectives for the TOE trace back to the threats in the security problem definition.

Table 5 - Rationale for Security Objectives of the TOE

Threats	Rationale
T.COMINT	The security objective below counters T.COMINT: • O.CRYPT will ensure that all cryptographic functions compliant to the relevant industry standards. All the data collected and transmitted by TOE using cryptographic algorithms is done so in compliance to standards and protected from attacks that attempt to bypass the security mechanisms of TOE • O.TOECOM ensures that the TOE protect the confidentiality of communications between distributed TOE components

T.DISCLOSURE	The security objective below counters T.DISCLOSURE: • O.AUTHENTICATE ensures that all users are authenticated before they access a protected resources or functions • O. KEYPROTECT ensures that all cryptographic keys stored within the TOE are protect sufficiently to prevent their disclosure to a malicious entity • O.CRYPT will ensure that all cryptographic functions compliant to the relevant industry standards. All the data collected and transmitted by TOE using cryptographic algorithms is done so in compliance to standards and protected from attacks that attempt to bypass the security mechanisms of TOE
T.IMPERSON	The security objective below counters T.IMPERSON: • O.AUTHENTICATE ensures the likelihood of a successful impersonation is reduced by the identification and authentication measures (username, passwords and 2FA code) • O.LOGGING ensures that all security-relevant action such as unauthorised login is logged and allow only TOE User to view them
T.PASSWORD	The security objective below counters T.PASSWORD: • O.PASSWORD ensures that all TOE users adhere with the acceptable password policy (minimum of 8 characters in length, at least 1 uppercase letter, 1 number, and 1 special characters) to avoid from unauthorised user taking advantage of weak password and gain unauthorised access to the TOE functions.

4.4.2 Security objectives rationale for the operational environment

The following table demonstrates that all security objectives for the operational environment are trace back to assumptions in the security problem definition.

Table 6 - Security objectives rationale for the operational environment

Objectives	Assumption	Rationale
OE.AUTHORISE OE.INSTALL	A.AUTHORISE	OE.AUTHORISE and OE.INSTALL fulfilled the assumption by ensuring the the TOE user assigned to operate the TOE is trusted by the organisation and are trained in use of the TOE and also download and install the TOE in accordance to the guidance document provided by the developer

Objectives	Assumption	Rationale
OE.OS OE.OPSYS	A.OS A.OPSYS	OE.OS and OE.OPSYS fulfilled the assumptions by ensuring that operating systems selected are of sufficient hardness to counter the perceived threats and the operating system on the underlying platform meet the minimum requirements for the TOE and updated prior to installation to provide underlying security to the TOE.
OE.UPDATE	A.OS A.UPDATE	OE.UPDATE fulfilled the assumptions by ensuring the TOE underlying operating system and application are updated on a regular basis.
OE.FIREWALL	A.FIREWALL	OE.FIREWALL fulfilled the assumption by providing network filtering at the gateway through configuration of HTTPS and HTTP defined by the organization.
OE.TIMESTAMP	A.TIMESTAMP	OE.TIMESTAMP fulfilled the assumption by ensuring that reliable timestamps are provided by the operational environment for the TOE.

5 Security Requirements (ASE_REQ.2)

5.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from Version 3.1 (REV 5) of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions used within this ST to depict their application:

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].
- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].
- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.
- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b.

5.2 Security Functional Requirements

5.2.1 Overview

The security functional requirements are expressed using the notation stated in Section 5.1 above and are itemised in the table below.

Table 7 - Security Functional Requirements

Identifier	Title
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FCS_CKM.1	Cryptographic key generation

Identifier	Title
FCS_CKM.2	Cryptographic key distribution
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FIA_ATD.1	User attribute definition
FIA_UID.2	User identification before any action
FIA_UAU.2	User authentication before any action
FIA_SOS.1	Verification of secrets
FMT_SMF.1	Specification of Management Functions
FTP_TRP.1	Trusted path

5.2.2 FAU_GEN.1 Audit data generation

Hierarchical to:	No other components.
FAU_GEN.1.1	The TSF shall be able to generate an audit report of the following auditable events: ~~a) Start-up and shutdown of the audit functions;~~ b) All auditable events for the [***not specified***] level of audit; and **c) [Specifically defined auditable event listed in the Notes section below].**
FAU_GEN1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**none**].
Dependencies:	FPT_STM.1 Reliable time stamps
Notes:	Auditable event within the TOE: • TOE User login and logout activities • Reset Password • Reset Password request

5.2.3 FAU_SAR.1 Audit review

Hierarchical to:	No other components.
FAU_SAR.1.1	The TSF shall provide [**TOE User**] with the capability to read [**all audit information**] from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.
Dependencies:	FAU_GEN.1 Audit data generation
Notes:	None.

5.2.4 FCS_CKM.1 Cryptographic key generation

<table>
<tr><td>Hierarchical to:</td><td>No other components.</td></tr>
<tr><td>FCS_CKM.1.1</td><td>The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [<b>cryptographic key generation algorithms specified in Table 8</b>] and specified cryptographic key sizes [<b>cryptographic key sizes specified in Table 8</b>] that meet the following: [<b>standards as specified in Table 8</b>].</td></tr>
<tr><td>Dependencies</td><td>[FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction</td></tr>
<tr><td>Notes:</td><td><b>Table 8 - Cryptographic Key Generation</b>
<table>
<tr><th>Algorithm</th><th>Key size</th><th>Standard</th></tr>
<tr><td>ECC</td><td>Prime256v1</td><td>FIPS186-4</td></tr>
<tr><td>ECIES</td><td>Prime256v1</td><td>FIPS186-4</td></tr>
<tr><td>ECDSA</td><td>Prime256v1</td><td>FIPS186-4</td></tr>
<tr><td>AES CBC</td><td>256</td><td>FIPS197</td></tr>
<tr><td>AES-256-CM-HMAC-SHA1-80</td><td>256</td><td>FIPS197</td></tr>
</table></td></tr>
</table>

5.2.5 FCS_CKM.2 Cryptographic key distribution

Hierarchical to:	No other components.
FCS_CKM.2.1	The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [**distribution of session keys using TLS**] that meets the following: [**none**]
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	None

5.2.6 FCS_CKM.4 Cryptographic key destruction

Hierarchical to:	No other components.
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**key zeroization**] that meets the following: [**none**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
Notes:	None

5.2.7 FCS_COP.1 Cryptographic operation

Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform [**cryptographic operations specified in Table 9**] in accordance with a specified cryptographic algorithm [**cryptographic algorithm specified in Table 9**] and cryptographic key sizes [**cryptographic key sizes specified in Table 9**] that meet the following: [**standards as specified in Table 9**]
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or

<table>
<tr><td></td><td>FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction</td></tr>
<tr><td>Notes:</td><td>
<b>Table 9 - Cryptographic Operation</b>
<table>
<tr><th>Operation</th><th>Algorithm and mode</th><th>Key size</th><th>Standard</th></tr>
<tr><td>Encryption and decryption</td><td>ECC</td><td>Prime256v1</td><td>FIPS186-4</td></tr>
<tr><td></td><td>ECIES</td><td>Prime256v1</td><td>FIPS186-4</td></tr>
<tr><td></td><td>ECDSA</td><td>Prime256v1</td><td>FIPS186-4</td></tr>
<tr><td></td><td>AES CBC</td><td>256</td><td>FIPS197</td></tr>
<tr><td></td><td>AES-256-CM-HMAC-SHA1-80</td><td>256</td><td>FIPS197</td></tr>
</table>
</td></tr>
</table>

5.2.8 FIA_ATD.1 User attribute definition

Hierarchical to:	No other components.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**Username, Password, 2FA Authentication Code**]
Dependencies:	No dependencies.
Notes:	None.

5.2.9 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.2.10 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification

FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	No dependencies.
Notes:	None.

5.2.11 FIA_SOS.1 Verification of secrets

Hierarchical to:	No other components.
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet [• **8 characters in length,** • **at least 1 uppercase letter,** • **at least 1 number, and** • **at least 1 special characters**].
Dependencies:	No dependencies.
Notes:	None.

5.2.12 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**Refer to Table 10 and Table 11**]
Dependencies:	No dependencies.
Notes:	**TOE Web Application**

Table 10 - TOE Web Application Operation

User Role	Menu	Operation
TOE User	Login	Sign In
		New? Sign Up Here
		Forget your password? Click Here
		Return To Home

	Profile	Edit Display Name (Edit Display Name, Enable/Disable 2FA)
		Change Picture
		Change Password
	Logout	Logout

TOE Software Application

Table 11 - TOE Software Application Operation

User Role	Menu	Operation
TOE User	Login	Sign In
		Free Sign Up
		Forgot Password?
	Meetings	Upcoming (Join)
		Host (Start, Edit, Delete)
		New Meeting (Meeting Title, Description (Optional), Schedule Time, Meeting Duration, Participant ID, Participants)
		History (Search Messages)
	Chat	View Chat Messages
		Reply Chat Messages
		Delete Chat Messages
		Forward Chat Messages
		Call Contact
		Search Messages
		Email
		Emoji

		File Attachment
		Send
	Contacts	Add Contact (Enter Email Address)
		Add Group (Enter Group Name, Select Participant)
		Contact (Call, Chat, Delete Contact)
		Group (Edit, Delete)
	Settings	Edit Profile (Change profile picture, Change password)
		Test Audio
		Test Video
		Upload File
		Download File
		View Login History
		About (Update)
	Logout	Logout

5.2.13 FTP_TRP.1 Trusted path

Hierarchical to:	No other components.
FTP_TRP.1.1	The TSF shall provide a communication path between itself and [***remote***] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [***modification or disclosure***].
FTP_TRP.1.2	The TSF shall permit [***remote users***] to initiate communication via the trusted path
FTP_TRP.1.3	The TSF shall require the use of the trusted path for [***initial user authentication***, [**and all further communication after authentication**]].

Dependencies:	No dependencies.
Notes:	None.

5.3 TOE Security Assurance Requirements

EAL2 requires evidence relating to the design information and test results, but does not demand more effort on the part of the developer than is consistent with good commercial practice.

EAL2 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description on the architecture of the TOE, to understand the security behaviours.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to attackers with basic attack potential.

EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_CMC.2 Use of a CM system
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction

Assurance class	Assurance components
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security Problem Definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.2 Independent testing - sample
	ATE_FUN.1 Functional testing
	ATE_COV.1 Evidence of coverage
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

5.3.1 Explanation for Selecting the SARs

The assurance package for the evaluation of the TOE is Evaluation Assurance Level 2 (EAL2). The TOE has a low to moderate level of assurance in enforcing its security functions when instantiated in its intended environment, which imposes no restrictions on assumed activity on applicable networks. EAL2 is sufficient to demonstrate that the TOE is resistant to attackers with a Basic attack potential.

5.4 TOE Security Requirements Rationale

5.4.1 Dependency Rationale

The table below demonstrates the mutual supportiveness of the SFRs for the TOE by demonstrating how the SFR dependencies are fulfilled by the TOE and by justifying those dependencies that are not fulfilled.

The SARs relevant to the TOE constitute an evaluation assurance level of EAL2, as defined in the Common Criteria and include no extensions or augmentations. Therefore, as a complete evaluation assurance level, they are a mutually supportive set and require no further justification.

Identifier	Dependency	Inclusion
FAU_GEN.1	FPT.STM.1	FPT_STM.1 has not been included as the TOE obtains all audit timestamps from the underlying platform/operational environment. This has been

Identifier	Dependency	Inclusion
		addressed in Section 3.4 by A.TIMESTAMP.
FAU_SAR.1	FAU.GEN.1	FAU.GEN.1
FCS_CKM.1	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	FCS_COP.1 FCS_CKM.4
FCS_CKM.2	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1 FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1]	FCS_CKM.1
FCS_COP.1	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1 FCS_CKM.4
FIA_ATD.1	No dependencies	N/A
FIA_UID.2	No dependencies	N/A
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_SOS.1	No dependencies	N/A
FMT_SMF.1	No dependencies	N/A
FTP_TRP.1	No dependencies	N/A

5.4.2 Mapping of SFRs to Security Objectives for the TOE

Objective	Rationale
O.LOGGING	This objective is met by: • FAU_GEN.1 specifying which events to log • FAU_SAR.1 allowing TOE User to read the log
O.AUTHENTICATE	This objective is met by: • FIA_UID.2 and FIA_UAU.2 specifying that users must be identified and authenticated before allowing access • FIA_ATD.1 ensures user security attributes are maintained. • FMT_SMF.1 lists the security management functions that must be controlled after TOE users are identified and authenticated
O.KEYPROTECT	This objective is met by: • FCS_CKM.1 which generates cryptographic keys in accordance with a specified cryptographic key generation algorithm • FCS_CKM.4 which destroys cryptographic keys in accordance with a specified cryptographic key destruction method. • FCS_COP.1 which performs cryptographic operation in accordance with a specified cryptographic algorithm
O.CRYPT	This objective is met by: • FCS_CKM.1 which generates cryptographic keys in accordance with a specified cryptographic key generation algorithm • FCS_CKM.4 which destroys cryptographic keys in accordance with a specified cryptographic key destruction method. • FCS_COP.1 which performs cryptographic operation in accordance with a specified cryptographic algorithm
O.TOECOM	This objective is met by: • FTP_TRP.1 which ensures that traffic transmitted between TOE components is protected from disclosure and modification • FCS_CKM.2 which distributes cryptographic keys in accordance with a specified cryptographic key distribution algorithm.
O.PASSWORD	This objective is met by: • FIA_SOS.1 specifying that the TOE user password has a minimum of 8 characters in length, at least 1 uppercase letter, 1 number, and 1 special characters

6 TOE Summary Specification (ASE_TSS.1)

6.1 Overview

This section provides the TOE summary specification, a high-level description of how the TOE implements the claimed security functional requirements. The TOE provides the following security functions:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Secure Communication

6.2 Security Audit

The TOE will generate audit logs (which contain the date and time of the event, type of event, name of the device, device IP address and outcome of the transaction event (success or fail)) for the following auditable events (**FAU_GEN.1**):

- TOE User login and logout activities
- Reset Password
- Reset Password request

The TOE users have the capability to view these audit records via the TOE software **(FAU_SAR.1)**. Timestamps for the TOE is generated by utilising the underlying operating system. The TOE does not generate its own timestamps for use in audit records; these are supplied by the underlying operating system.

6.3 Cryptographic Support

The TOE performs key generation, encryption and decryption using ECC (P256v1), ECIES (P256v1), ECDSA (P256v1), AES256 CBC Mode and AES-256-CM-HMAC-SHA1-80 cryptographic algorithm with Prime256v1 and 256 bits cryptographic key sizes (**FCS_CKM.1, FCS_COP.1**). The TOE also able to destroy cryptographic keys by performing key zeroization (**FCS_CKM.4**).

- During user registration, the TOE generates Elliptic Curve Cryptography (P256v1) for TOE users

- The TOE encrypts the private keys using AES 256 CBC Mode

- The TOE encrypts the chat messages (including chat messages during online meeting) using AES256 CBC Mode, ECIES P256v1, ECDSA P256v1

- The TOE encrypts the file attachment during chat messaging (including file attachments during online meeting) using AES256 CBC Mode, ECIES P256v1, ECDSA P256v1

- The TOE performs the encryption for video/voice call using SRTP AES-256-CM-HMAC-SHA1-80

The TOE distributes the session keys using TLS (**FCS_CKM.2**). Distribution of session keys occurred during the TLS handshake with the Vidcall server. The TOE perform authentication of TLS packets and shared the TLS authentication key.

6.4 Identification and Authentication

The TOE maintains only 1 type of user role which is TOE users. As stated in Section 1.6.1, the TOE consists of two parts; TOE web application and TOE software application. The TOE web application is used by the TOE users to perform TOE users registration, change TOE users password, enable two-factor (2FA) authentication. The TOE software application (installed on the TOE users workstation) is used to perform TOE operation such as video conferencing, audio conferencing, Audio/Video peer to peer call, screen sharing, chat and messaging, meeting recording, watermark, file sharing and history.

TOE users are required to be identified and authenticated before any information flows are permitted (**FIA_UAU.2, FIA_UID.2**). The TOE software application can be downloaded by the TOE user by visiting to https://1dataonline.com/home/homepage. On the homepage, simply click the "Download" button to download the installer necessary for installation. At the login page (for both TOE web and software application), TOE users need to key in a valid username and password in order to access the TOE (**FIA_ATD.1**). The acceptable password should be at least 8 characters in length and should include at least 1 uppercase letter, 1 number, and 1 special characters (**FIA_SOS.1**). TOE users have the option to enable the two factor authentication (2FA). 2FA can be enabled by login to the TOE web application (https://1dataonline.com/authentication/Login). 2FA can be authenticated through email authentication. By default, 2FA authentication is implemented by email 6 digit code number to user email. In this case, the 6 digit code will be emailed to user after successful enter username and password (**FIA_ATD.1**)

The TOE operations include (**FMT_SMF.1**):

TOE Web Application

User Role	Menu	Operation
TOE User	Login	Sign In
		New? Sign Up Here
		Forget your password? Click Here

		Return To Home
	Profile	Edit Display Name (Edit Display Name, Enable/Disable 2FA)
		Change Picture
		Change Password
	Logout	Logout

TOE Software Application

User Role	Menu	Operation
TOE User	Login	Sign In
		Free Sign Up
		Forgot Password?
	Meetings	Upcoming (Join)
		Host (Start, Edit, Delete)
		New Meeting (Meeting Title, Description (Optional), Schedule Time, Meeting Duration, Participant ID, Participants)
		History (Search Messages)
	Chat	View Chat Messages
		Reply Chat Messages
		Delete Chat Messages
		Forward Chat Messages
		Call Contact
		Search Messages
		Email
		Emoji
		File Attachment
		Send

	Contacts	Add Contact (Enter Email Address)
		Add Group (Enter Group Name, Select Participant)
		Contact (Call, Chat, Delete Contact)
		Group (Edit, Delete)
	Settings	Edit Profile (Change profile picture, Change password)
		Test Audio
		Test Video
		Upload File
		Download File
		View Login History
		About (Update)
	Logout	Logout

6.5 Secure Communication

The TOE provides trusted paths for communication with remote users that is logically distinct from other communication channels. These trusted paths protect transmitted data from disclosure and undetected modification. All remote communications take place over a secure encrypted session which involve (**FTP_TRP.1**):

- TLS v1.2 is a cryptographic protocol that ensures privacy between communicating applications and users on the Internet. TLS is commonly used to secure data transmission over a computer network. TLS v1.2 includes features like strong encryption algorithms, message authentication codes, and key exchange methods to ensure the confidentiality and integrity of data during transmission.

- SRTP Secure Real-time Transport Protocol. An extension of Real-time Transport Protocol (RTP) that features enhanced security measures. The protocol provides encryption, confidentiality, message authentication, and replay protection to your transmitted audio and video traffic using AES-256-CM-HMAC-SHA1-80

- OAuth 2.0 Bearer Tokens are a security mechanism used to authenticate and authorize access to resources on a web server. These tokens are commonly used in conjunction with RESTful

APIs (Representational State Transfer APIs) to ensure secure and controlled access to protected resources.