ENEX.
CARBON

SECURITY CLAIMS ASSESSMENT

DEKKO Secure

Version 2.0

Carbon Security Pty Ltd - 274 Victoria Street, Brunswick, Victoria 3056

t. +61 3 9436 7454 I w. enexcarbon.com.au

Mailing Address PO Box 219 Brunswick, VIC 3056 Australia

ABN: 95 614 877 753

1 Background

DEKKO Secure supplies their product to a number of key clients, including Government, who require independent validation of security claims.

2 Scope

- This document (*independent report*) can be provided to prospective clients and details:
  - The vendor, DEKKO Secure, stated security claims of the product
  - The methodologies and references used to assess those claims
  - The assessment results *(PASS/FAIL)*
  - The assessment outcomes
  - Any relevant observations
- This document (*independent report*) provides assurance to prospective clients that the DEKKO product security claims have been validated by an independent third-party.

3 Summary

The DEKKO environment was found to adhere to good security practice with regards to information transport security, access control, authorisation and availability. The environment is subject to ongoing security development with respect to OWASP (Open Web Application Security Project) community standards and MITRE Common Weaknesses standards and guidelines. Baseline security testing of the DEKKO environment found no significant actionable issues at the date of this assessment *(August 2018).*

4 A.8 DEKKO Secure CLAIMS *(ICD - Initial Claims Document)*

This section details the security functionality claims of the DEKKO Secure product

Claim Ref	Claim Statement	ASSESSMENT
C1	Only the owner of the account has access to the unshared messages, chats, and files stored in their account.	PASS

4.1 Claims Assessment:

The DEKKO application environment uses a username and password, with optional multi-factor authentication. After authentication, users are assigned a session identifier (cookie).

The authentication component was tested for known weaknesses such as default credentials, caching issues and password reset functionality, in accordance with the OWASP Testing Guide (v4).

The authentication credentials are never transmitted to DEKKO and are processed locally in browser using the Stanford JavaScript Crypto Library to sign messages and authenticate the user, using a combination of password and a public/private key. The resulting hash of this combination is used to verify and authorise users within the DEKKO environment.

The session identifier and state management features within the application were tested and found to adhere to accepted industry standards to ensure users are correctly segregated and authorised to view files, chats and messages.

4.2 Security Standards Referenced:

OWASP A5.2017 - Broken Access Control https://www.owasp.org/index.php/Top_10-2017_A5-Broken_Access_Control

Mitre CWE 285 - Authorization Weaknesses

https://cwe.mitre.org/data/definitions/285.html

4.3 Testing Methodology:

https://www.owasp.org/index.php/Testing_for_authentication

https://www.owasp.org/index.php/Testing_for_Authorization

https://www.owasp.org/index.php/Testing_for_Session_Management

Claim Ref	Claim Statement	ASSESSMENT
C2	Only people designated to see shared material (files, messages) can see them unencrypted.	PASS

4.4 Claims Assessment:

Transport security was tested and found to adhere to industry good practices. All services in scope were found to receive A+ security rating for transport security by Qualys SSL Labs.

The DEKKO application environment uses a username and password, with optional multi-factor authentication. After authentication, users are assigned a session identifier (cookie).

The authentication component was tested for known weaknesses such as default credentials, caching issues and password reset functionality, in accordance with the OWASP Testing Guide (v4).

The authentication credentials are never transmitted to DEKKO and are processed locally in browser using the Stanford JavaScript Crypto Library to sign messages and authenticate the user, using a combination of password and a public/private key. The resulting hash of this combination is used to verify and authorise users within the DEKKO environment.

The session identifier and state management features within the application were tested and found to adhere to accepted industry standards to ensure users are correctly segregated and authorised to view files, chats and messages.

4.5 Security Standards Referenced:

OWASP A5.2017 - Broken Access Control https://www.owasp.org/index.php/Top_10-2017_A5-Broken_Access_Control

OWASP A3.2017 - Sensitive Data Exposure https://www.owasp.org/index.php/Top_10-2017_A3-Sensitive_Data_Exposure

Mitre CWE 311-Encryption of Sensitive Data
https://cwe.mitre.org/data/definitions/311.html

Mitre CWE 285 - Authorization Weaknesses

https://cwe.mitre.org/data/definitions/285.html

4.6 Testing Methodology:

https://www.owasp.org/index.php/Testing_for_authentication

https://www.owasp.org/index.php/Testing_for_Authorization

https://www.ssllabs.com/ssltest/analyze.html?d=DEKKO.io

Claim Ref	Claim Statement	ASSESSMENT
C3	No mechanism exists for others to get access to unencrypted data.	PASS

4.7 Claims Assessment:

Transport security was tested and found to adhere to industry good practices. All services in scope were found to receive A+ security rating for transport security by Qualys SSL Labs.

The DEKKO application environment uses a username and password, with optional multi-factor authentication. After authentication, users are assigned a session identifier (cookie).

The authentication component was tested for known weaknesses such as default credentials, caching issues and password reset functionality, in accordance with the OWASP Testing Guide (v4).

The authentication credentials are never transmitted to DEKKO and are processed locally in browser using the Stanford JavaScript Crypto Library to sign messages and authenticate the user, using a combination of password and a public/private key. The resulting hash of this combination is used to verify and authorise users within the DEKKO environment.

The session identifier and state management features within the application were tested and found to adhere to accepted industry standards to ensure users are correctly segregated and authorised to view files, chats and messages.

4.8 Security Standards Referenced:

OWASP A5.2017 - Broken Access Control https://www.owasp.org/index.php/Top_10-2017_A5-Broken_Access_Control

Mitre CWE 285 - Authorization Weaknesses

https://cwe.mitre.org/data/definitions/285.html

4.9 Testing Methodology:

https://www.owasp.org/index.php/Testing_for_authentication

https://www.owasp.org/index.php/Testing_for_Authorization

https://www.owasp.org/index.php/Testing_for_SSL-TLS_(OWASP-CM-001)

Claim Ref	Claim Statement	ASSESSMENT
C4	The shared materials (messages, files) are guaranteed to originate from the sharing user.	PASS

4.10 Claims Assessment:

The DEKKO application environment uses a username and password, with optional multi-factor authentication. After authentication, users are assigned a session identifier (cookie).

The authentication component was tested for known weaknesses such as default credentials, caching issues and password reset functionality, in accordance with the OWASP Testing Guide (v4).

The authentication credentials are never transmitted to DEKKO and are processed locally in browser using the Stanford JavaScript Crypto Library to sign messages and authenticate the user, using a combination of password and a public/private key. The resulting hash of this combination is used to verify and authorise users within the DEKKO environment.

The session identifier and state management features within the application was tested and found to adhere to accepted industry standards to ensure users are correctly segregated and authorised to view files, chats and messages.

DEKKO employs the use of secp256r1ECC Elliptic Curve Cryptography for end-to-end encryption and client-side management of cryptographic validation and identification.

4.11 Security Standards Referenced:

OWASP A3.2017 - Sensitive Data Exposure https://www.owasp.org/index.php/Top_10-2017_A3-Sensitive_Data_Exposure

OWASP A5.2017 - Broken Access Control https://www.owasp.org/index.php/Top_10-2017_A5-Broken_Access_Control

Mitre CWE 311-Encryption of Sensitive Data
https://cwe.mitre.org/data/definitions/311.html

Mitre CWE 285 - Authorization Weaknesses

https://cwe.mitre.org/data/definitions/285.html

4.12 Testing Methodology:

https://www.owasp.org/index.php/Testing_for_authentication

https://www.owasp.org/index.php/Testing_for_Authorization

https://www.owasp.org/index.php/Testing_for_Session_Management

Claim Ref	Claim Statement	ASSESSMENT

C5	There is only one way to restore access to an account without knowing the password: the trusted users.	PASS

4.13 Claims Assessment:

The DEKKO application environment uses a username and password, with optional multi-factor authentication. After authentication, users are assigned a session identifier (cookie).

The authentication component was tested for known weaknesses such as default credentials, caching issues and password reset functionality, in accordance with the OWASP Testing Guide (v4).

The authentication credentials are never transmitted to DEKKO and are processed locally in browser using the Stanford JavaScript Crypto Library to sign messages and authenticate the user, using a combination of password and a public/private key. The resulting hash of this combination is used to verify and authorise users within the DEKKO environment.

The session identifier and state management features within the application were tested and found to adhere to accepted industry standards to ensure users are correctly segregated and authorized to view files, chats and messages.

4.14 Security Standards Referenced:

OWASP A3.2017 - Sensitive Data Exposure https://www.owasp.org/index.php/Top_10-2017_A3-Sensitive_Data_Exposure

OWASP A5.2017 - Broken Access Control https://www.owasp.org/index.php/Top_10-2017_A5-Broken_Access_Control

Mitre CWE 311-Encryption of Sensitive Data
https://cwe.mitre.org/data/definitions/311.html

Mitre CWE 285 - Authorization Weaknesses

https://cwe.mitre.org/data/definitions/285.html

4.15 Testing Methodology:

https://www.owasp.org/index.php/Testing_for_authentication

https://www.owasp.org/index.php/Testing_for_Authorization

5 Document Information

Date	Version	Name	Description
24/08/2018	0.1	JM	Draft
27/08/2018	1.0	MJ	Review
30/08/2018	2.0	MT	Final