Cisco App Center - App Export Compliance Questionnaire

Developer/Partner Name:

Haystack Networks Ltd

Address:
6 Granger Row
Chelmsford
Essex
Contact Number:
07968 763 986

Contact Email address:
simon.birtles@haystacknetworks.com
aciappcenter-support@haystacknetworks.com

Export Questionnaire and Responses

Export laws require that Apps containing encryption be properly authorized for export. Failure to comply could result in severe penalties. Developers posting to Cisco App Headquarters are responsible for obtaining required government approvals.
For further information, click here: http://www.bis.doc.gov/encryption/default.htm

1. Does your App contain encryption of any type such as SSL, SSH, HTTPS, VPN, IPSEC, AES, 3DESetc.)?
   HTTPS to the locally resident APIC Webserver on TCP/443

2. Does your App contain, use or make calls to encryption for any purpose other than authentication or anti-virus protection (such as encryption used for secure network management, HTTPS, VPN, or wireless security)?
   HTTPS to the locally resident APIC Webserver on TCP/443

3. Does your App contain, use or make calls to encryption for any purpose other than piracy and theft prevention for software?
   Yes - The app uses HTTPS (TLS) for calls to the co-resident Cisco APIC as the APIC requires HTTPS by default.

4. Does your App contain, use or make calls to encryption greater than 64-bit symmetric or greater than 1024-bit asymmetric algorithms? **HTTPS as above - TLS 1.2 (a strong protocol), ECDHE_RSA with P-256 (a strong key exchange), and AES_256_GCM (a strong cipher).**

5. Does your App contain, use, or access encryption for protection of data or information security purposes?
   Yes - The app uses HTTPS (TLS) for calls to the co-resident Cisco APIC as the APIC requires HTTPS by default.

Please describe the encryption used in your App and the type of information it secures, e.g. network management data, user data,

The app uses HTTPS (TLS) for calls to the co-resident Cisco APIC as the APIC requires HTTPS by default. This secures all data transfer between the co-resident application and Cisco APIC application.

6. Do any of the following describe your App or a feature or function of your App? Check all that apply.

_____ A) App that provides or performs "non-standard cryptography" such as WAPI, or other proprietary encryption means

_____ B) An application-specific software development kit using cryptography.

_____ C) A cryptographic library, development kit or toolkit

_____ D) App that provides or performs vulnerability analysis, network forensics, or computer forensics

_____ E) App that provides or performs investigation of data leakage, network breaches, and other malicious intrusion activities through triage of captured digital forensic data an example is CALEA

_____ F) App providing secure Wide Area Network (WAN), Metropolitan Area Network (MAN), Virtual Private Network (VPN), satellite, digital packet telephony/media (voice, video, data)

_____ G) App designed, modified, adapted or customized for government end-user(s) or with cryptographic functionality that has been modified or customized to customer specification;

_____ *H)* App with cryptographic functionality or encryption components (except encryption software that is publicly available) that is user-accessible and can be easily changed by the user;

_____ I) App with an open cryptographic interface or a means for a user to insert cryptographic functionality without assistance;

_____ J) App providing cryptanalysis or cryptanalytic functions ;

__√__ **K)None of the above criteria apply.**

Name:
Simon Birtles

Title:
Author & Company Director

Signature:

Date:
05-10-2017