ads.cert Call Signs Protocol

Specification

January 2022

注意：

本ドキュメントは、IAB Tech Lab が公開しているドキュメントを簡易的に翻訳したものです。正確な情報は、下記オリジナルドキュメントを参照してください。

https://iabtechlab.com/wp-content/uploads/2021/09/2-ads-cert-call-signs-pc.pdf

© 2022 IAB Technology Laboratory

目次

© 2022 IAB Technology Laboratory

Program Leaders:

Curtis Light, Staff Software Engineer - Google

Rob Hazan, Senior Director, Product - Index Exchange

Other Significant Contributions from:

Ben Antier, CEO - Publica

Nabhan El-Rahman, CTO - Publica

Joshua Gross, Senior Engineering Lead - Index Exchange Bret Ikehara, Staff Software Engineer, Publica

Johnny Li, Software Engineer, Index Exchange

Amit Shetty, Programmatic Products & Partnerships - IAB Tech Lab Sam Mansour, Principal Product Manager - Moat

Miguel Morales, CTO & Co-Founder - Lucidity Tech

Colm Geraghty, Principal Architect - Verizon Media Group Mani Gandham, Engineering - Index Exchange

James Wilhite, Director of Product management, Publica

IAB Tech Lab Lead:

Amit Shetty

VP, Programmatic Products & Partnerships - IAB Tech Lab

About IAB Tech Lab(IAB Tech Lab について)

IAB Technology Laboratory(Tech Lab)は、効果的で持続可能なグローバルデジタルメディアエコシステムの成長を促進するための標準、ソフトウェア、サービスを制作・提供する非営利の研究開発コンソーシアムです。デジタルパブリッシャーやアドテクノロジー企業、マーケター、広告代理店、その他インタラクティブマーケティング分野に関心のある企業で構成される IAB Tech Lab は、透明で安全かつ効果的なサプライチェーン、よりシンプルで一貫性のある測定、消費者にとってより良い広告体験を通じて、ブランドとメディアの成長を可能にすることを目指し、モバイルと TV/デジタルビデオチャネルの実現に焦点を当てています。IAB Tech Lab のポートフォリオには、消費者、パブリッシャー、広告主、サードパーティープラットフォームのデジタル体験を改善するために設計された DigiTrust リアルタイム標準化 ID サービスが含まれています。ボードメンバーには、AppNexus、ExtremeReach、Google、GroupM、Hearst Digital Media、Integral Ad Science、Index Exchange、LinkedIn、MediaMath、Microsoft、

Moat、Pandora、PubMatic、Quantcast、Telaria、The Trade Desk、ヤフージャパンが含まれます。2014 年に設立された IAB Tech Lab は、ニューヨークに本部を置き、サンフランシスコにオフィス、シアトルとロンドンに支部を置いています。

IAB Tech Lab の詳細はこちら: www.iabtechlab.com

Getting Started(はじめに)

ads.cert または Call Signs プロトコルを初めて使用する場合は、ads.cert 入門から始めることをお勧めします。この入門書は、プロトコルスイートの概要と、さまざまな広告技術のユースケースのセキュリティ確保における暗号の役割に関する入門的な資料を提供しています。

Objective(目的)

本ドキュメントでは、広告技術参加者(バイヤー、セラー、仲介者、またはベンダーなど)固有のビジネス識別子を確立する目的で、ads.cert Call Sign インターネットドメイン名を作成するプロセスについて説明します。ads.cert 仕様は、このドメイン名を使用する他の広告技術参加者に公開鍵を配布するため、DNS に依存しています。ads.cert プロトコルスイートの他の認証プロトコルは、通信で ads.cert Call Sign ドメインを提供することで、相手に対して参加者を識別します。これにより、さまざまな広告技術のユースケースで標準化された公開鍵の配布が可能になります。

DNS はそれ自体では安全でないプロトコルであるため、ある種の DNS 脅威ベクトルから保護する手段として、DNSSEC を使用するようにこのドメインを設定するためのガイドラインを提供します。

Protocol

Internet domain name(インターネットドメイン名)

ads.cert Call Sign は、DNS 構成が周知のサブドメインの下で特定の標準化レコードをホストするインターネットドメイン名です。実装会社（example.com など）によって登録された”Public Suffix + 1”(PS+1)ドメイン名（publicsuffix.org によって公開されている）下の DNS レコード名” _adscert”は、この周知の DNS サブドメイン階層のルートを表します。この目的で有効なのは、ICANN が割り当てたサフィックスのみです。publicsuffix.org ファイルの"private"セクションの使用はサポートされていません。

© 2022 IAB Technology Laboratory

拡張文字セットドメインを人間が解釈しようとしますと、かなりのセキュリティリスクを伴うため、このプロトコルでは、ASCII 文字セット内の counterparty ads.cert Call Sign ドメインを使用する必要があります。このスキームに参加するローカライズされたドメインは、正規表現として Punycode 形式で表現されなければなりません。ドメイン名自体に加えて、これは DNS レコードコンテンツ(すでに ASCII に制限されている)および署名メッセージにも適用されます。ドメインを ASCII 文字に制限することで、拡張文字をサポートすることで可能になるソーシャルエンジニアリングから保護しながら、広告エコシステム内の最も幅広い利用者がアクセスできるようにできます。

Domain Name System Security Extensions (DNSSEC) compatibility (ドメインネームシステムセキュリティ拡張（DNSSEC）の互換性)

インターネットのパイオニアたちは、1980 年代初頭に DNS プロトコルを作成しましたが、その前にプロトコルを保護する必要があることが明らかになりました。その 10 年以上後、DNSSEC は、DNS レコードの内容を認証し、DNS キャッシュポイズニングなどの攻撃を防止するために、DNS レコードの内容に静的な署名を提供するプロトコルとして登場しました。

現在、DNS レコードを保護するための最も適切なソリューションですが、DNSSEC は独自の複雑さとリスクをもたらします。ほとんどの主要なオンラインプロパティは、DNS ベースの攻撃からウェブトラフィックを保護するために DNSSEC に依存していません。なぜなら、DNSSEC はウェブブラウザ/オペレーティングシステムで採用されている CA/Browser Forum の認証局モデルによって冗長化されたソリューションだからです。
このため、HTTPS で保護されたウェブサイトがドメインに DNSSEC を利用しているのを見かけることは通常ありません。DNSSEC は、比較的堅牢な(別途問題があるわけではないにせよ)CA ソリューションの上に追加的なセキュリティをほとんど提供せず、これは DNSSEC ベースの停止に関連する停止リスクに見合うものではありません（例）。

しかし、私たちは、DNSSEC が以下のような DNS のみのプロトコルスイートに適していると信じています。ads.cert のような DNS のみのプロトコルスイートでは、DNSSEC の役割があると考えます。ads.cert コールサインドメインの DNS ゾーンは、DNSSEC レコードの生成を有効にするように設定することを推奨します(ただし、必須ではありません)。ads.cert の DNS レコードは、それらを消費する必要があるシステムによってキャッシュされることを意図しているため、特定のドメインの DNSSEC(または他の形式の DNS 停止)が、基礎となるプロトコルの運用を実質的に中断させることはないはずです。

ads.cert を採用する事業者が DNSSEC ドメインを使用するかどうかを決定するのは自由です。採用する場合は、この目的に専用または適した新規または既存の“vanity”ドメイン名を使用することを推奨します。

Public key record name and format(公開鍵レコードの名前と形式)

ads.cert スイートの各種プロトコルは、異なる公開鍵形式を必要とする場合があるため、必要なサブドメインおよびレコードのレイアウト、ならびに ads.cert Call Sign の使用法の詳細は、各 ads.cert 認証プロトコルを参照してください。

Implementation Recommendations(実施に関する推奨事項)

ID ドメインの確立、秘密鍵/公開鍵の生成、および DNS 経由での公開鍵の公開について説明している、この仕様書に付属する実装者ガイドを参照してください。

© 2022 IAB Technology Laboratory