ads.cert Primer

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/2021/09/1-ads-cert-primer-pc.pdf

目次

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

Introduction(はじめに)

IAB Tech Lab の ads.cert プロトコルスイートは、プログラマティック広告エコシステムにオープンスタンダードの暗号セキュリティ基盤を提供します。これらのソリューションを使用することで、参加者は虚偽表示から保護された本物の広告取引機会を確実に得られます。広告取引の売買や促進を行うあらゆる関係者は、無料の ads.cert ツールとプロトコルを広告配信環境に導入できます。参加者は、この仕組みの中で、自動的かつ確実にお互いを発見します。その連合体化された性質により、広告内のビジネスアイデンティティの裁定者となる中央当局は存在しません。

ads.cert プロトコルは、プログラマティック広告を購入/販売/促進する企業に焦点を当てています。あらゆる形態の消費者プロファイル識別子は完全に対象外です。ads.cert とエンドユーザー識別子/Cookie を混同しないでください。

私たちプロトコルスイートを 2 つの主要なコンセプトに分類します:

- ある広告エコシステム参加者のビジネス ID を、公開鍵を配布する標準的な方法を使用して、 他の参加者に正式に指定する方法。
- 特定の広告ユースケースにセキュリティを追加するために、この公開鍵配布基盤を活用する個々の認証プロトコル。

提供されるオープンソースソフトウェアソリューションは、公開鍵の配布とセキュリティプロトコルの両方のプロセスを容易にします。

Background: cryptography concepts(背景:暗号の概念)

ads.cert を理解するために、まず通信セキュリティを支えるいくつかの概念を要約します。ads.cert オープンソースソフトウェアが実装していますが、ドキュメント全体を通してこれらの用語に言及してい

ます。

- **Private key(秘密鍵)**: 秘密鍵は非常に大きな(256 ビット、または 1 の後に 77 桁続く)ランダムな数値で、推測が難しく他人に知られてはいけません。この秘密値を持つ人なら、それを公開することなく、特別な数学的公式を使って、自分がその値を知っていることを証明できます。
- **Public key(公開鍵)**: 公開鍵は、別の 256 ビットの数値で、標準的な公式を使って秘密鍵から計算されます。この計算はコンピュータにとって簡単です。公開鍵の値は誰にでも安全に配布できます。公開鍵を持っている人が、そこから生成された元の秘密鍵を解読することは事実上不可能です。
- **Key Exchange(鍵交換)**: 鍵交換は、お互いに秘密鍵を持つ 2 人が、他の人にその秘密がわからないように、お互いに秘密を合意する技術です。アリスとボブがそれぞれ自分の公開鍵を公開している場合を考えましょう。アリスは数学的公式を使って自分の秘密鍵とボブの公開鍵を組み合わせ、共有秘密値を求めます。ボブも同様の公式を使って自分の秘密鍵とアリスの公開鍵を組み合わせ、同じ共有秘密値を求めます。この共有秘密値は、どちらかの秘密鍵を持たない第三者が知ることはできません。
- **MAC: Message Authentication Code(メッセージ認証コード)**: メッセージ認証コード(MAC)は、秘密とメッセージを組み合わせて、メッセージを提供する人がその秘密を知っていて、メッセージが改ざんされていないことを証明する番号を作成するための公式です。本来の秘密を知らないと、本物の MAC とランダムな数字を見分けることはできません。

これらのコンセプトは、現代のすべての安全な通信(この文書を読むために使用している技術を含む)の基礎となっています。

Identifying Businesses That Use Programmatic Advertising (プログラマティック広告を利用する企業の特定)

ads.cert プロトコルは、他の広告エコシステム参加者が公開鍵を見つけ、鍵交換やメッセージ認証プロセスで使用できるように、公開鍵を配布するための標準的な方法を提供します。このプロセスを簡素化するため、ドメインネームシステム(DNS)を使用して公開鍵を配布します(ちょうど DNS がウェブサイトに関連する IP アドレスを通信するように)。これが最初の ads.cert 固有のプロトコルコンセプトで

す。

ads.cert Call Sign は、ads.cert 参加事業者が DNS を使用して公開鍵を公開するインターネットドメイン名です。事業者はその後、他のさまざまな ads.cert 認証スキーム内で対応する秘密鍵を使用して、アクティビティを実行する事業者の身元を表明できます。これにより、参加事業者が互いを安全に識別するための暗号基盤が提供されます。どの当事者も、新規または既存のドメインの下に必要な DNS レコードを作成するだけで、ads.cert Call Sign を作成できます。

例えば、架空のビジネス(”Fictional Ads LLC”)は、自社のサービスのマーケティング(real-fictional.com.ex)や広告配信(fictional-serving.com.ex)に使用するさまざまなインターネットドメインを持っているかもしれません。ガイドラインに従い、Fictional Ads は、**ads.cert Call Sign** として使用するための独自のインターネットドメイン名(fictional-ads-llc.com.ex)を設定します。_adscert.fictional-ads-llc.com.ex サブドメイン内で、このビジネスは、他のエコシステム参加者にビジネスの活動を認証するために使用される公開鍵を含む DNS レコードを公開します。

さまざまなプログラマティック広告の相互作用の中で、Fictional Ads は、他の当事者がビジネスを自動的に識別して認証できるように、正式に fictional-ads-llc.com.ex として自己宣言します。

この情報だけでは、ドメインの DNS 管理者が DNS の公開鍵に対応する秘密鍵を所有していることを証明するためにしか使用できません。誰でも簡単にインターネットドメイン名(無料のものも含む)を登録し、必要な DNS レコードを公開し、わずか数分で ads.cert スキームに完全に参加できます。これだけでは、ビジネスの識別と認証ツールに過ぎず、ビジネスの広告活動を審査するための外部プロセスを追加する必要があります。

しかし、これによって得られるのは、ビジネスと結びついた強固な認証ソリューションの上に、広告活動を取り巻く外部のレビュー、監査、認証プロセスを重ねるための強力なツールです。

- コンソーシアム、認定機関(TAG、MRC など)、およびその他の広告品質審査機関は、事業者を特定するための信頼できるキーとして、認証レジストリ内の事業者の ads.cert Call Sign を活用できます。これにより、加入者は、特定の監査済み参加者から発信された活動であることを確認するための直接的な手段を得られるため、このようなデータソースはさらに有用なものとなります。また、このようなグローバルおよび地域的なコンプライアンス組織にまたがる一意のビジネス識別子ス

キームが作成されます。

- 広告バイヤー自身の内部レビューとリスク管理プロセスにより、自動化を改善し、長期にわたって活動の期限を保証できます。

ads.cert Call Sign(正式に割り当てられた地上波/海上/航空無線送信所の用語にインスパイアされたネーミング)は、業界全体で使用される明確かつ普遍的な概念になると信じています。

この公開鍵配布スキームを使用することで、プログラマティック広告のライフサイクルのさまざまな段階を通じて認証を追加できます。

Securing direct, server-to-server communications (サーバー間の直接通信の保護)

ads.cert Authenticated Connections プロトコルは、サーバー間のクリエイティブフェッチやインプレッション ping など、データセンター間で発生する広告関連の HTTP リクエストを認証します。これは、互いに直接的な契約関係にない当事者間(サーバーサイドのアドインサーションプラットフォームやデマンドサイドプラットフォームなど)において、最大のメリットをもたらします。

実装者は、ads.cert オープンソースソフトウェアを使用して、(ads.cert Call Sign で)リクエストを発信するビジネスを識別する認証 HTTP リクエストヘッダーを生成します。このヘッダーは、URL と HTTP リクエストボディも認証します。このプロトコルは、標準的なハッシュ化メッセージ認証コード(HMAC)アルゴリズムを使用して、規模や帯域幅の要件を減らしながら効率的に署名を計算します。

これは、パブリックコメントとベータテスト期間が完了すれば、一般に使用できる最初の ads.cert 認証プロトコルとなります。

Securing bid requests, bids, and ad delivery (ビッドリクエスト、ビッド、広告配信の保護)

私たちのワーキンググループは、リアルタイムビッドプロトコルの改ざんを防ぐことに焦点を当てた、次のスキームの草案を作成しています。**ads.cert Authenticated Delivery** プロトコルは、セラーにリアルタイムフィードバックを提供し、デマンドソースや下流の関係者がプログラマティックバイヤーに

ビッドリクエストを誤って伝えていないことを確認します。さらに、広告配信の結果として落札されたビッドは、特定のセラーがビッドリクエストの当初の主張通り、インプレッションの配信に実際に参加したことをバイヤーに認証します。ads.cert オープンソースソフトウェアの将来のリリースでは、このプロトコルのサポートが含まれ、基盤となる公開鍵配布インフラを活用する予定です。

Authentication suitable for advertising(広告に適した認証)

よくある質問：なぜ ads.cert は単に公開鍵署名アルゴリズムを使わないのでしょうか？このアプローチなら、よりシンプルなプロトコルを提供でき、署名者が受信者の公開鍵を入手する必要もありません。私たちがこのルートを選択しなかった理由には、主に 2 つの考慮点があります。

第一に実用的です。公開鍵署名アルゴリズムは、比較的複雑度の低い HMAC アルゴリズムよりも計算コストが高いです。ビッドリクエスト処理のような頻度の高いユースケースでスキームをスケーラブルに保つために、より効率的なオプションを選択することを優先しました。

しかし、より重要なのは耐久性の問題です。公開鍵署名を入手した人は誰でもそれを検証できます。プライバシーと目的外の使用を防ぐために、私たちは署名スキームを意図的に設計し、排他性と対称性を持たせています。
署名は、意図された受信者だけに限定されます。他の当事者は、鍵交換から共有された秘密を持っていませんので、他の当事者は署名と乱数を区別できません。また、発信者と受信者の双方が共有秘密を持っているため、どちらかが署名を作成することも可能です。この受信者の"偽造可能性の抜け穴"は、どのような署名の真正性に関しても、発信者にもっともらしい反証可能性を与えます。

Community-driven, open source software
(コミュニティ主導のオープンソースソフトウェア)

ads.cert の各実装者が低レベルのプロトコルを一から扱うことを要求するのではなく、その代わりに、IAB Tech Lab がホストする、コミュニティ主導の、ads.cert インフラストラクチャとプロトコルのプロダクションクオリティの実装を構築することに重点を置いています。数台のアプリケーションサーバーから大規模なサーバーまで、あらゆる規模の組織のニーズを考慮しています。

コアコンポーネントは Go ソフトウェア言語を使用して構築され、リモートプロシージャコールのインテグレーションオプションにより、幅広いホスト環境へのインテグレーションが可能です。私たちは、

さまざまなベストプラクティスを用いて、一般的な環境に安全に導入しやすいソリューションを作ることに重点を置いて設計しました。モニタリング、障害リスクの軽減、その他のプロダクション化に関する懸念は、インテグレーションと活用に最小限の労力で済むよう、完全なソリューションの中で対処しています。コア・プロトコルの仕様もパブリッシャーとして公開しますが、ほとんどの参加者は既製のソリューションを活用することを好むと思います。