Ads.cert - Authenticated Devices

Executive Summary

Ads.cert is a collection of standards designed to help cryptographically secure the digital advertising ecosystem against misrepresentation of ad opportunities. This document focuses specifically on attestation of the authenticity of the device and app on which an ad opportunity is being presented.

Business Problem

In digital advertising, device and app information presented in ad opportunities is used by buyers in the bidding process. This information is seller-provided and is subject to misrepresentation by sellers and intermediaries in the supply chain. Low-value ad opportunities can thus be misrepresented as high-value, as seen in various streaming TV fraud operations detected in recent times (citation required). In addition to misrepresenting device information, bad actors are also known to generate fake traffic outright, generating ad opportunities from thin air using bots that masquerade as myriad devices and apps (citation required).

While device and app misrepresentation is a particularly attractive exploit vector for streaming TV owing to the high CPMs, the threat vector exists for other devices as well, such as smart speakers that can play audio ads, digital signage, personal computers, smartphones, etc. Without a mechanism to validate that ad traffic is indeed coming from the device and app it claims to be from, such misrepresented traffic will be hard to identify and will continue to result in wasted ad spend for advertisers and lost monetization for legitimate publishers.

In the above, ad traffic refers to client-originated traffic employed for programmatic advertising purposes, such as bid requests, impression notifications, rich media events, etc.

Out of scope

On-device placement misrepresentation: Since this standard operates at a device-level granularity, misrepresentation of ad opportunities within the device and / or app itself are out of scope. Placement misrepresentation, a form of ad fraud that involves misrepresenting ad placements so that they appear as higher-value, is one such example. Bad actors are known to misrepresent display ad placements as video ad placements by generating a fake video ad request from the display ad placement (citation required). The ad opportunity will seem as if it's coming from a genuine device and app, which it is; however, the mechanism of generating the opportunity is what is illegitimate.

Specific Project Requirements

This section outlines the various functional and non-functional requirements that need to be met by proposals, stack-ranked by importance.

Functional requirements

1. Enable on-demand attestation of device and app information in ad traffic so that recipients don't have to blindly trust seller-provided information.
2. Enable independent verification of attestations so that recipients can gauge the authenticity of the associated transaction.
3. Enable aggregation of device attestation data at a seller level so that enforcement actions may be taken.
4. Enable support for disparate device types and user agents such as streaming TV (Advanced TV) devices, audio devices, smartphones, tablets, desktops, web browsers, etc. MVP may be Advanced TV if others are not feasible to include.

Non-functional requirements

1. Protect against attacks such as replay forgery or context transplanting. Keep certain context (pixel firings) tied to the device that's being shown
2. Except for device manufacturer attestation processes where the device manufacturer uses a persistent identifier to identify requests coming from a specific device over a period of time, no identifier should leave the device that can be used to correlate the device's content consumption activities with a specific device or consumer profile.
3. The attestation verification process should not interrupt the bidding process or the creative delivery process so that user experience is not adversely impacted.
4. Attestations should be non-repudiable so that verifiers can trust the integrity and durability of attestations across the lifecycle of the attestation.
5. Implementers should be able to support distinct versions of the protocol so that future releases do not break existing implementations.
6. Leverage established and well-tested cryptographic mechanisms and frameworks as much as possible to reduce the potential for exploits.
7. The proposed mechanism should support all popular device manufacturers within the supported device type. This assumes that mechanisms may be distinct across device types: the mechanism used for desktop device attestations may be distinct from the mechanism used for streaming TV devices.
8. The impact of a compromise of any on-device keys this mechanism relies on should not extend beyond that set of devices. Essentially, learning a secret key used by a set of devices should not result in other devices being impacted, so that the blast radius of the compromise is limited.
9. The verification mechanism should align with existing verification models employed by marketers, such as using independent verification vendors to measure and report on the quality of their ad campaigns.

10. Client applications that generate ad opportunities should not require changes to support this standard, since updating apps causes considerable churn.
11. Attestations should have a limited life so that a non-repudiable cryptographic record of consumer or business activity is not generated and stored.
12. Independent verification of signatures should not require a round trip to the device or the attester so that latency is minimized.
13. Proposed mechanisms should not require publisher/developer support to implement, so that it is not dependent on adoption by parties that have a vested interest to not support the mechanism.
14. Since advertising systems operate under stringent latency requirements, creating attestations and verifying attestations should not be resource-intensive operations.
15. The attestation mechanism should be durable across device software and hardware updates so that availability of attestation data is not impacted over time.
16. Proposals should minimize dependencies on other transparency standards (especially standards like Authenticated Delivery) since it can potentially hinder adoption of this standard.
17. While this standard focuses on abating device and app misrepresentation, proposals should allow for flexibility so that use cases presently deemed out of scope can be supported in the future.

Intended usage

The intent of this standard is to reduce ad fraud by making it harder for bad actors in the supply chain to misrepresent device and app information in ad traffic. As the web moves relentlessly towards securing user privacy, third-party access to stable/persistent identifiers will be inevitably restricted. Indeed, having access to such identifiers, even if for legitimate fraud-detection purposes, may become a liability considering regulatory concerns. A side-effect of not having stable identifiers is that mechanisms like device-specific deny lists can no longer be leveraged. Consequently, enforcement actions would likely need to be taken at a seller-level, with implementer-specific policies applying.

Since coverage of attestation data is unlikely to reach 100%, there are likely to be three classifications within total measured ad traffic:

1. Valid attestations
2. Invalid attestations
3. Unsupported

Implementers may choose to set enforcement thresholds for these classifications at different granularities of suppliers (publisher, reseller, exchange, etc.) or demand partners (DSPs, ad servers, etc.).

Practical considerations

While there may be proposals that meet the functional and non-functional requirements outlined above, there may be practical considerations that prevent adoption. These may pose a risk to the eventual success or durability of the Authenticated Devices standard and proposals should outline how these practical considerations are accounted for.

Support from device manufacturers

It is likely that proposals will require some form of implicit trust in device manufacturers to be able to attest to the authenticity of their devices. Some device manufacturers may be less agreeable to implementing support for a device attestation mechanism for the ads industry than others. Such device manufacturers may command a large market share, so it would make sense to support any existing attestation mechanisms they provide to maximize supported device coverage. For example, Google has the Play Integrity API, which provides the following attestations: (i) Genuine app binary; (ii) Genuine Play installation on the device; (iii) Genuine Android device. Apple provides the DeviceCheck API, which enables devices to be marked as genuine and provides genuine app attestations as well. Apple has also launched support for Private Access Tokens, a protocol that as of this writing is going through the IETF standards track.

Lack of centralized trust models

It is common for certain types of devices, such as smartphones, to have a centralized trust model that enables third parties to enshrine trust in the device manufacturer for device attestation. However, there are devices that operate in a wholly decentralized manner, sometimes by design. Proposals that have fallback mechanisms for attestation by parties other than the device manufacturer may achieve better coverage, albeit at lower levels of trust. One could imagine that in future iterations of the protocol some trust models may be preferred by buyers over others, the standard will strive to be transparent in each model allowing for that decisioning.

Interplay with upcoming privacy standards

Proposals should consider the potential impact of upcoming privacy standards, such as initiatives under Google's Privacy Sandbox[1], on the efficacy of the proposed attestation mechanism. There are also multiple privacy-related proposals being discussed in various W3C community groups. These proposals lean on the W3C Privacy Principles[2] for a consistent privacy posture. Proposals that do not account for these privacy principles could find themselves incompatible with the underlying browser or device implementation in the future, risking the durability of this standard.

[1] https://privacysandbox.com/
[2] https://www.w3.org/TR/privacy-principles/

Performance

Since attestation mechanisms are likely to require multiple hops between parties and will require computational resources on the client, ad traffic recipients should have verification policies that are mindful of the impact on customer experience. Recipients can request attestations for a small but meaningful sample of overall ad traffic to gain the necessary intelligence required for enforcement at a seller level.

Limitations

Lack of a persistent seller ID

Without persistent device / user identifiers, it is even more important to have a persistent representation of a seller ID that is consistent across the digital advertising industry so that enforcement actions don't become a game of whac-a-mole. However, no such persistent representation exists today, which will make it harder to share threat intelligence with the industry around which sellers are misrepresenting devices.

Working Group

Security Foundations Working Group

Working Group Approval

Meeting Date which project proposal was reviewed.
If it came to a vote - note the votes by company for record

Project Timeline

To be completed by WGO upon project approval. Proposed project timeline based on when the solution may be needed in market.

Step	Week of Aug 25	Week of Sept 8	Week of Sept 22	Week of Oct 6	Week of Oct 20	Week of Nov 3	Week of Nov 17
Proposals/Discussion	Finalize scope						
Revision							

Decision							
PC Release							Prep Doc

Proposals Submitted

Links to proposal docs

Proposal	Owner	Summary