iab. TECH LAB

ads.cert Call Signs Protocol Specification

January 2022

Presented by the IAB Tech Lab Cryptographic Security Foundations working group

Please email support@iabtechlab.com with feedback or questions. This document is available online at https://iabtechlab.com/standards/ads-cert/

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

The IAB Technology Laboratory (Tech Lab) is a non-profit research and development consortium that produces and provides standards, software, and services to drive growth of an effective and sustainable global digital media ecosystem. Comprised of digital publishers and ad technology firms as well as marketers, agencies, and other companies with interests in the interactive marketing arena, IAB Tech Lab aims to enable brand and media growth via a transparent, safe, effective supply chain, simpler and more consistent measurement, and better advertising experiences for consumers, with a focus on mobile and TV/digital video channel enablement. The IAB Tech Lab portfolio includes the DigiTrust real-time standardized identity service designed to improve the digital experience for consumers, publishers, advertisers, and third-party platforms. Board members include AppNexus, ExtremeReach, Google, GroupM, Hearst Digital Media, Integral Ad Science, Index Exchange, LinkedIn, MediaMath, Microsoft, Moat, Pandora, PubMatic, Quantcast, Telaria, The Trade Desk, and Yahoo! Japan. Established in 2014, the IAB Tech Lab is headquartered in New York City with an office in San Francisco and representation in Seattle and London.

Learn more about IAB Tech Lab here: www.iabtechlab.com

TABLE OF CONTENTS

Getting Started

If you're new to ads.cert or the Call Signs protocol, we recommend starting with the *ads.cert Primer*. It provides an overview of the protocol suite and some introductory materials regarding the role of cryptography in securing various advertising technology use cases.

Objective

This document describes the process of creating an ads.cert Call Sign Internet domain name for the purpose of establishing an advertising technology participant (e.g. a buyer, seller, intermediary, or vendor) unique business identifier. Our ads.cert specification relies on DNS for distributing public keys to other ad technology participants using this domain name. Other authentication protocols in the ads.cert protocol suite identify the participant to counterparties by providing the ads.cert Call Sign domain in communications. This allows standardized public key distribution for various advertising technology use cases.

Because DNS on its own is an unsecured protocol, we provide guidelines for configuring this domain to use DNSSEC as a means for protecting against certain forms of DNS threat vectors.

Protocol

Internet domain name

An ads.cert Call Sign is an Internet domain name whose DNS configuration hosts specific standardized records under a well-known subdomain. The DNS record name "`_adscert`" under the "public suffix + 1" (PS+1) domain name (as published by publicsuffix.org) registered by the implementing company (e.g. example.com) represents the root of this well-known DNS subdomain hierarchy. Only ICANN-assigned suffixes are valid for this purpose. Use of the "private" section of the publicsuffix.org file isn't supported and implementers should ignore any of these encountered.

Due to the considerable security risks involved with humans trying to interpret extended character set domains, our protocols require use of counterparty ads.cert Call Sign domains within the ASCII character set. Any localized domain participating in this scheme must be expressed in Punycode format as a canonical representation. In addition to the domain name itself, this applies to DNS record content (already limited to ASCII) and signature messages. Limiting domains to ASCII characters helps keep them accessible to the broadest audience within the advertising ecosystem while protecting from social engineering that's possible through supporting extended characters.

Domain Name System Security Extensions (DNSSEC) compatibility

Internet pioneers created the DNS protocol in the early 1980s before it became evident that the protocol needed to be secured. Over a decade later, DNSSEC emerged as a protocol to provide static signatures over the content found in DNS records to authenticate their content and prevent attacks such as DNS cache poisoning.

While currently the most appropriate solution for securing DNS records, DNSSEC introduces its own complexity and risk. Most major online properties do not rely on DNSSEC for securing web traffic against DNS-based attacks because it's largely a solution that's made redundant by the CA/Browser Forum's certificate authority model adopted by web browsers/operating systems. This is why you typically won't find HTTPS-secured websites utilizing DNSSEC for their domain: it provides little additional incremental security on top of the relatively robust (if not also separately troubled) CA solutions, and this isn't worth the outage risks associated with DNSSEC-based outages (examples).

We do believe, though, that DNSSEC has its place in a DNS-only protocol suite such as ads.cert. We recommend (but do not require) that the ads.cert Call Sign domain's DNS zone be configured to enable generation of DNSSEC records. The ads.cert DNS records are meant to be cached by systems that need to consume them, so a DNSSEC (or any other form of DNS outage) for a particular domain should not materially disrupt the operation of underlying protocols.

It is up to the business adopting ads.cert to decide whether they want to use a DNSSEC domain. If elected, we suggest using a new or existing "vanity" domain name that can be dedicated or suitable for this purpose.

Public key record name and format

Because various protocols in the ads.cert suite may require different public key formats, refer to the specific ads.cert authentication protocol for more information about the required subdomain and record layout, and their usage of ads.cert Call Signs.

Implementation Recommendations

Please refer to the *Implementer's Guide* that accompanies this spec document which walks through establishing an identity domain, generating private/public keys, and publishing public keys via DNS.