# fTLD Registry Services

## DMARC for Public Suffix Domains
## ICANN73 - Tech Day

March 7, 2022

# Introduction

- fTLD operates .BANK and .INSURANCE as trusted, verified and more secure TLDs; security and brand protection are top priorities
- Advantageous to consider security hierarchically (i.e., what's possible at the TLD level such as inclusion on the HSTS preload list)
- fTLD Security Requirements include Email Authentication and are monitored and enforced for compliance
  - Domains used to send email must have DMARC (and be at reject within 90 days of deployment) and SPF; we also advocate DKIM
  - Domains in the DNS, but not used for email must have DMARC at reject
- Extending DMARC 'above' organizational domains (e.g., example.bank) would protect non-existent domains, enforce compliance with the requirement and provide threat intelligence to mitigate DNS Abuse

# DMARC Refresher

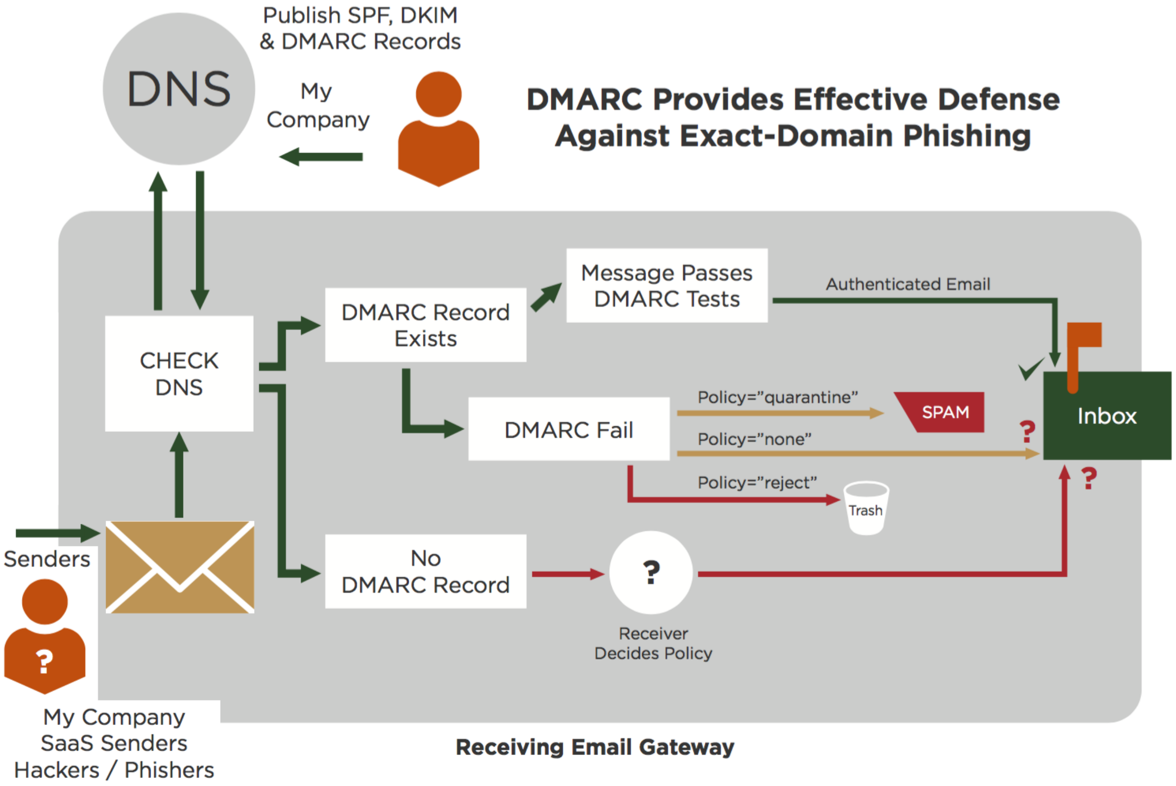
DNS based protocol layered on top of well-established email authentication technologies

- SPF (2005)
- DKIM (2007)

Produces policy results

- Pass
- Fail, reject
- Fail, spam folder
- Fail, report only

Feedback to sending orgs



# DNS Records Example

- fTLD.com
  - **DMARC:** v=DMARC1; p=reject; rua=mailto:dmarc_agg@vali.email
  - **DKIM:** v=DKIM1; k=rsa; p=MIGfMA0G ...
  - **SPF:** v=spf1 include:_spf.google.com ip4:205.201.128.0/20 ip4:198.2.128.0/18 ip4:209.15.212.47 ip4:52.36.33.222 include:servers.mcsv.net ip4:165.22.46.120 ip4:148.105.0.0/16 ip6:2604:a880:800:c1::2b2:c001 -all

# Public Suffix Domain (PSD) DMARC

- PSDs include TLDs where the organizational domain starts at a lower level (e.g., .gc.ca, .gov.uk, .police.uk)
- Simple extension to DMARC for additional public suffix lookup:
  - ○ **Extend DMARC ‘above’ organizational domains for a limited namespace**
  - ○ Where DMARC is required
  - ○ Registries with control of SLDs in their namespace (e.g., .Brands, .gov, .mil)
  - ○ Only for PSDs defined in new “registry”; see concept at http://psddmarc.org/
- Add explicit policy for non-existent domains (usually np=reject)
- Feedback data in DMARC reports
  - ○ Minimize potential privacy considerations by limiting access to data

# Path Forward

- After three years of work IETF RFC 9091 was published in July 2021
- As a follow-on effort, integrate with IETF RFC 7489 update (i.e., DMARC), 2022+
- ICANN authorization for select gTLDs to publish records
- Work with mail service providers (e.g., Microsoft, Google) to implement PSD DMARC
- Brand (e.g., Amazon, Microsoft) and other trusted/verified TLD operators have expressed support; others are likely interested
- Significant stakeholder engagement underway; concept has been well received and there’s still work to do
- PSDs such as .gov.uk and .mil have DMARC records and synthesized the mail service provider role to validate results

# Issues

- Requires publication of DMARC record for TLDs
  - **Not an issue for ccTLDs (_dmarc.gov.uk published now) and other non-ICANN TLDs (.gov, .mil)**
  - **Informal RSEP submitted to ICANN in August 2021 for discussion; PSD DMARC prohibited in Base Registry Agreement**
- No technical risk
  - No root DNS changes (uses _dmarc.TLD)
  - gTLD deployment technically equivalent to _dmarc.gov and _dmarc.mil, which have been without issues
- Policy consideration for privacy issues associated with reporting
  - **Constrain PSD to TLDs that meet appropriate technical and policy criteria (DMARC required)**
  - **Progress for gTLD use pending ICANN authorization**

# Summary

- PSD DMARC extends DMARC coverage to mitigate DNS Abuse and improve brand protection
- Technical approach defined by IETF in RFC 9091
- Good feedback from initial deployment by ccTLDs and non-ICANN TLDs
- Technical approach low risk for expanding to gTLDS
- Need ICANN policy/guidance for usage with appropriate gTLDs

# Information

- fTLD DMARC Working Group has included: Agari, Bank Policy Institute, Canadian Centre for Cyber Security (.gc.ca), Cybersecurity and Infrastructure Security Agency (.gov), dmarcian, Global Cyber Alliance, LinkedIn, Microsoft, National Cyber Security Centre (.gov.uk), Proofpoint, Universal Postal Union (.POST), U.S. Department of Defense (.mil), valimail and financial sector members
- PSDs interested: .bank, .gc.ca, .gov, .gov.uk, .insurance, .mil, .police.uk
- Look up DMARC and SPF records at EasyDMARC: https://easydmarc.com/
- Contact:
    - **Craig Schwartz, craig@fTLD.com**