Mutual Declaration Mechanism of Multi-provider Relationship for Trusted Web Services

IETF116 Yokohama 2023/03/28

Wataru Ohgai, Takao Kondo, Korry Luke, Satoshi Kai, Keisuke Uehara, Satoru Tezuka
Keio University
alt@sfc.wide.ad.jp

What M2DMRT does?

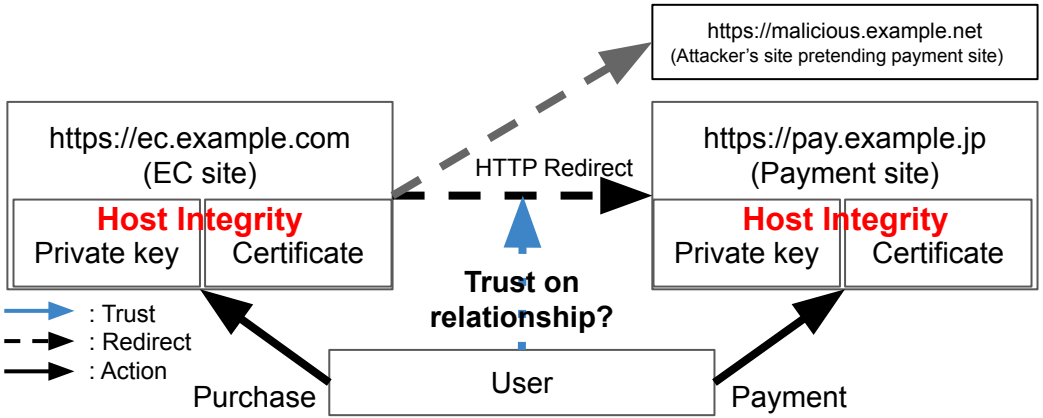
M2DMRT

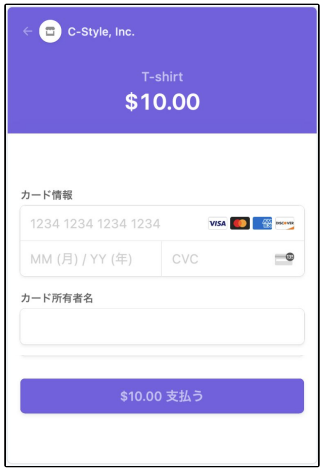
Mechanism of Mutual Declaration
of Multi-provider Relationship for Trusted Web services

Purpose	Contribution	Approach
Declaration and verification of redirect relationship of multiple SPs	Light-weight, self-manageable declaration of trust using digital signature of opponent TLS public key	- Declaration of relationship using DNSSEC - Mutual declaration by related SPs

TLS based security and redirection

- Security of Web is based on integrity assurance of hosts by TLS server certificate.
- Backend structure is being more complex, resulting in composing single Web service over multiple service providers (SPs) [5][6]
- This research focuses on the threat model regarding trust on multiple SPs' relationship when redirecting service traffic.

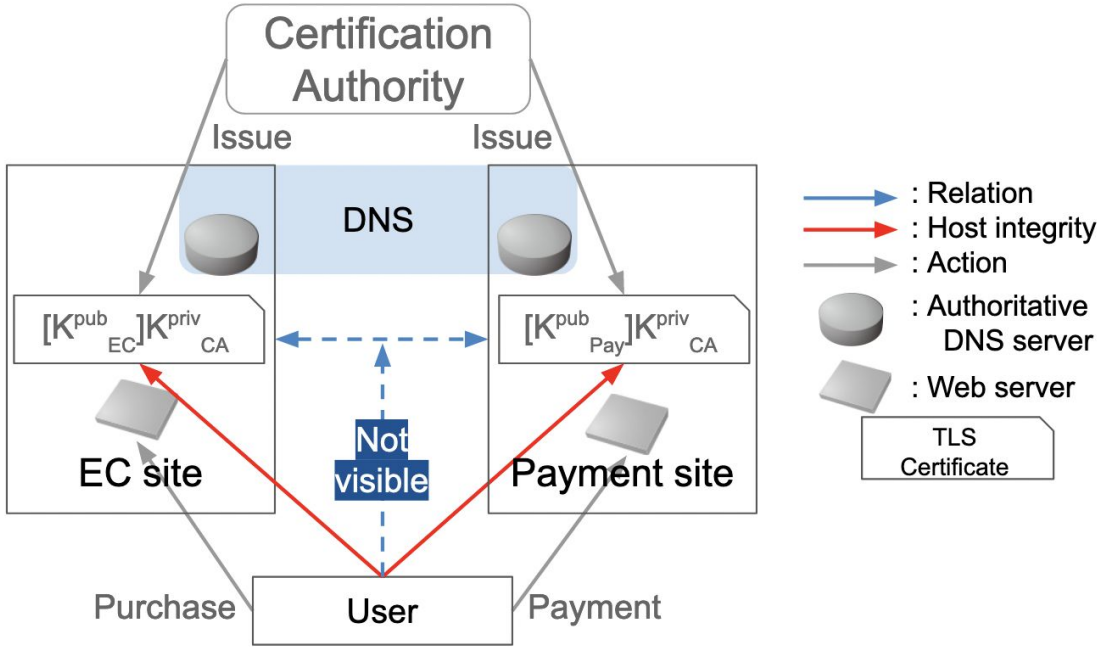




Problem statement

Integrity of single Web service containing multiple hosts/domain names

1. The host integrity is not always same as the service integrity.
2. TLS only assures the host integrity.[8][9][10][11][12][13]



Requirements

1. **Mutual** and **verifiable** declaration of service relationship
2. **Self-manageable** declaration of service relationship
3. **Minimum disclosure** of each party's components

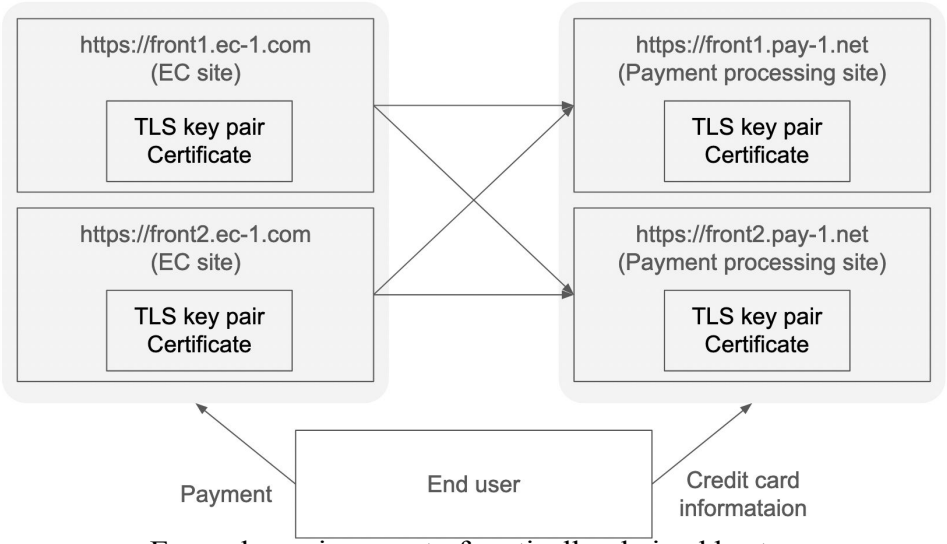
Against the threat model

4. **Localization of transaction** of declaration modification
5. **Localization/minimization of failure points** (independent from central authority)

System requirements

Requirements against feasibility

6. Adoption to the **Vertically-chained** Environment
7. Adoption Potential in **Horizontally-chained** Environments
8. Minimal **Processing Time** of Modification



Example environment of vertically-chained hosts.

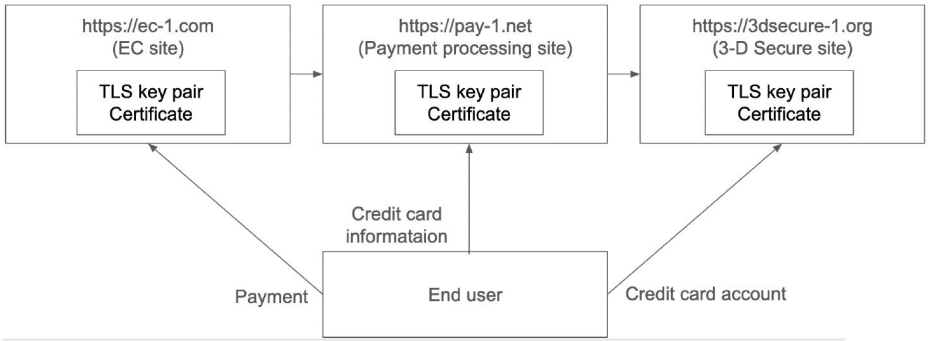
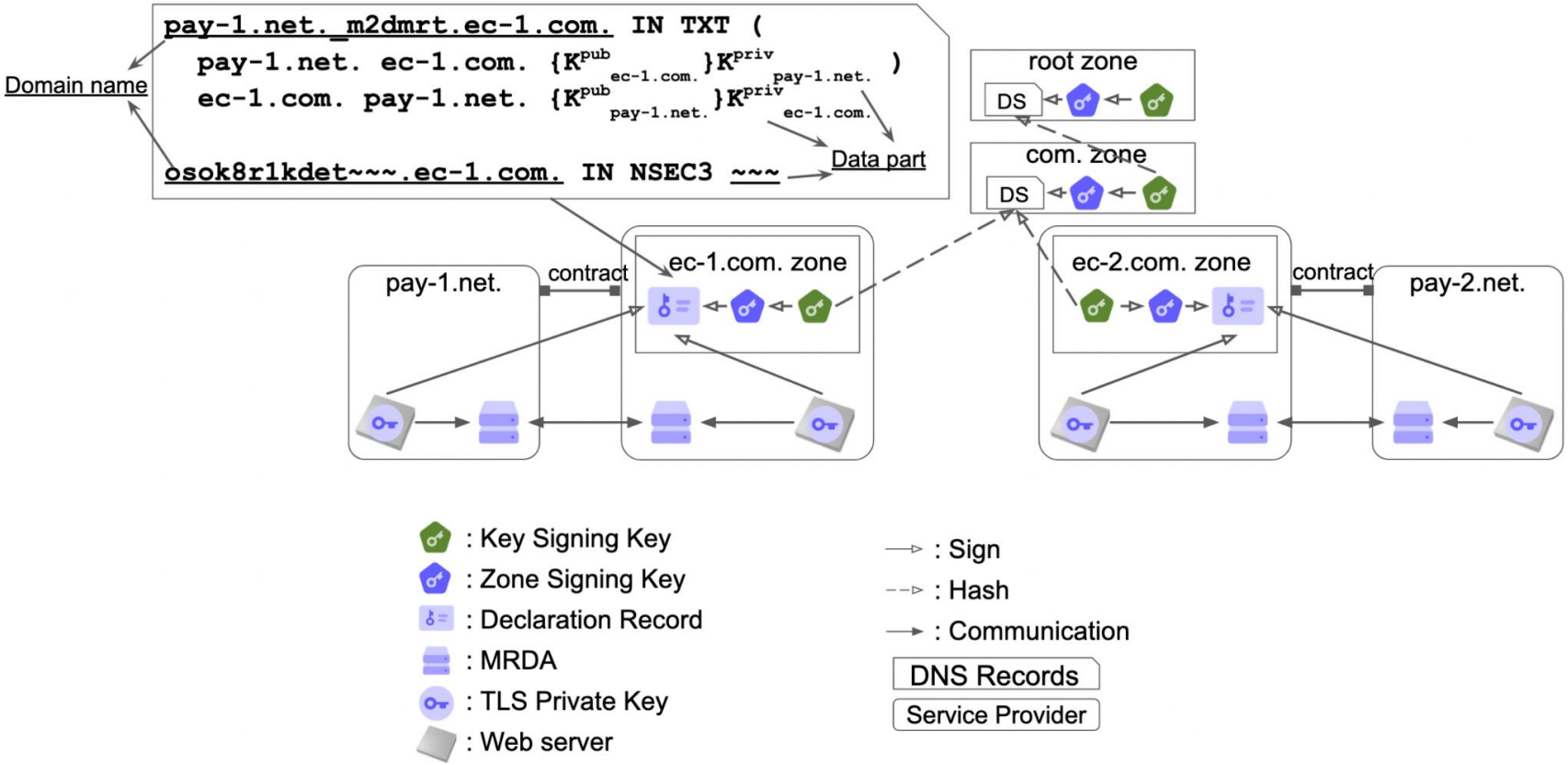


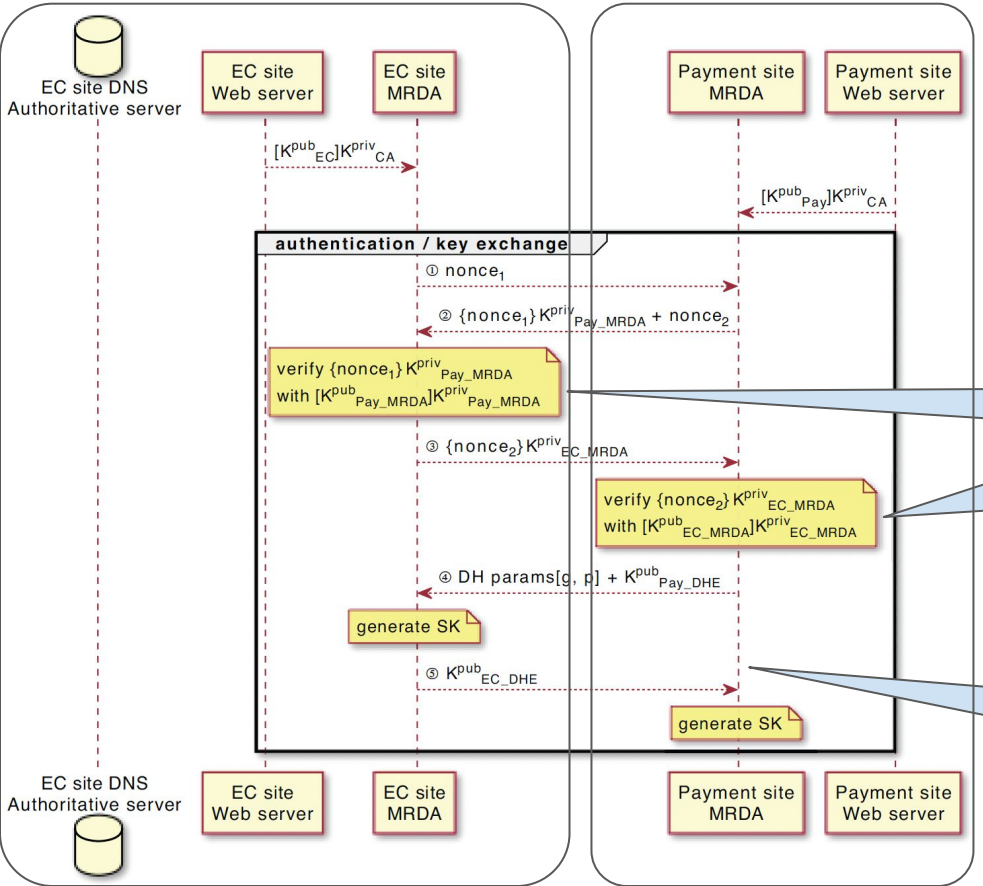
Fig. 2.1: Example environment of horizontally-chained hosts.

Proposal: M2DMRT



Registration sequence (1)

MRDA: Mutual Relation Declaration Agent



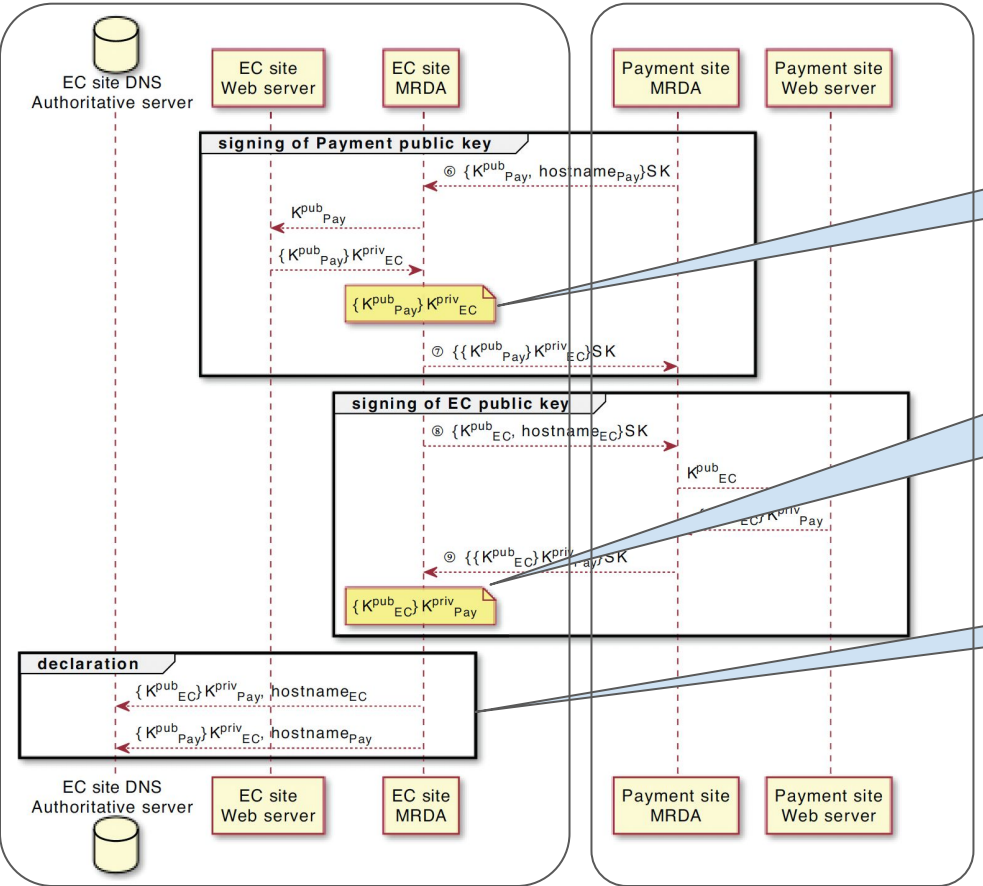
Authenticates the opponent MRDA to register

EC site's MRDA authenticates payment site's MRDA

Payment site's MRDA authenticates EC site's MRDA

Generates shared key using DHE kex
→Encrypts lasting communications with AES

Registration sequence (2)



Generates signature against payment site's pubkey

Generates signature against EC site's pubkey

Publish signatures as DNS records
→Mutual declaration

Declaration record

{dest_web}._m2dmrt.{origin_web}. IN TXT {signer_fqdn} {target_fqdn} {signature}

```
pay.exp.jj1lfc.dev._m2dmrt.ec.exp.jj1lfc.dev. 300 IN TXT "ec.exp.jj1lfc.dev. pay.exp.jj1lfc.dev. b'ZO+32YTS0uJ2kdtxa9/O
kYLKk1H7hl8hKLwIHiTv2rY1ptap9kyYuyDGlflp5lM1emKqHu0FhPPj/3AKesK4+nOgUzRdKFSmkKBqU/FsBU3VjySAslQq4zdoOR0ijnrW/3pBqCwW5H/
BzPz1gD/mDUaRgbH4+UD5zHA8fxikkFjUg7jxAAnLP7bzRncC3Z3qsui4mywxeYRnXQ6Qh6OL" "ajRWfIV1h1RFnCXegdReVfz2R5SEt04nqCUCZ/EeA6a
tOhNt5TCPiLGSG57+vkpcD6LpcKMK+lkcc36oBaqpfKFBLcnZ3Z3VFvdmlodA55Co3StIuot64s5b3S5/iweq/6BEUxxWIcb9djGHwc3Dyv+d4BHHaue5p0
9/KVUhRKj5Jjkz86qSWAh8qrvFHLLK96YGIwBGV+LnU7SpBbVrbQvZSAFd8E4pSj8vwqrurGeoO2lkA7Mnf695bQTKkT" "+2tssMd7UmZNscOwIoaXilSP
wzZlGiiYlglteeCh54oNSKrSivzIC6J3C9kDqYFvWcLncEEy5QiRLYW7y6wXRBBlyyy86LCC/6k8+Wen8HTIMmYw8pvJII724Dqqnk1/SHzLsYBAantP6iY
gBp+BjrVyZv7zoT8Go9DVMp6dcCqOywmaAGruVJJj9xbtwmmsGH2c34eefdWl4Coo8ZAW0t0='"
pay.exp.jj1lfc.dev._m2dmrt.ec.exp.jj1lfc.dev. 300 IN TXT "pay.exp.jj1lfc.dev ec.exp.jj1lfc.dev. b'iBVAK/KhGphWM3xOdeUg
mxnTmE8HvA16y2weU+c+gBlx78Xzl8fqBIgsMv4f+HPWSGr0fFo+IVwd75kHR79ePSt1uvGwMYnKOeTXSCXQWd8eO+35gZJ36pEhhrVtsRJi93MZFoMDYI3
vOnQHjyOMD+n4aMcdncssjlkNPzNL+G2muYXWT+66aT//Zs5e6b3tro3F3KNw77uZn83hqSZm" "jRaM3ebcp918osIiI2TK5CJNQO7ddXlyj4es0PsXuU3
4FJAqsn6vtLJKiYk0QECBbJg1lU6ev+ZFmkjC2+B7afvsfnKA3ZBBiX185e2B+zVkq0bAdIo8HsmoY3C0DLx0xMHfyJMjwgrro941TkxtnEGjgdb1fDv+0E
nOWelqlGWEnTzLL8V+PlbejpLoIFWoyrMw5ghOLfROcSqrs/8KyI+xiXSD4G5H1idFTxsIpowQcibWqsY9QluD3HVqmb" "IoBa+W2dNmCbuOK44sXc9Kur
8seSIJl2sn0ttlgzCTmTlVV258HPxLCSRN+L+RGYwdf9aZsQymRb3Yq8kn1nphBzyuYsRJyA7FQmm80v8Xq74gefMaveZqydwM4FQLApuuZnNr1QftkDiK5
IFU8n2bfpqVAJ7QZJWRqBpcN4UomgmO+ozpn04xr8Xc0P/WTi2ruq30o3gQy/naagwwBux6CtM='"
pay.exp.jj1lfc.dev._m2dmrt.ec.exp.jj1lfc.dev. 300 IN RRSIG TXT 13 9 300 (
                                20220210123947 20220127110947 10814 exp.jj1lfc.dev.
                                g2/7PIgTs3mg6skS1dNWWPiC4K1vfmBpU/R9Lip+jJb7
                                U1VjBcgLeeSg9gsEJ7h0ne3Vo61d3PzqngYQ3IqdsQ== )
```

DNSSEC signed

References

[5] 3-D Secure - EMVco. https://www.emvco.com/emv-technologies/3d-secure/.

[6] J. Zhao, P. Liang, W. Liufu, and Z. Fan. Recent Developments in Content Delivery Network: A Survey. In Parallel Architectures, Algorithms and Programming, pp. 98–106. Springer Singapore, 2020.

[8] M. Marlinspike. New Tricks For Defeating SSL In Practice. In Proc. of BLACKHAT Europe ’09, 2009.

[9] X. Li, C.Wu, S. Ji, and R. Gu, Q.and Beyah. HSTS Measurement and an Enhanced Stripping Attack Against HTTPS. In Security and Privacy in Communication Networks, pp. 489–509. Springer Intl. Pub, 2018.

[10] M. Zhang, X. Zheng, K. Shen, Z. Kong, C. Lu, Y. Wang, H. Duan, S. Hao, B. Liu, and M. Yang. Talking with Familiar Strangers: An Empirical Study on HTTPS Context Confusion Attacks. In Proc. of ACM CCS’20, pp. 1939–1952, 2020.

[11] J. Selvi. Bypassing HTTP Strict Transport Security. In Proc. of BLACKHAT Europe ’14, 2014.

[12] S.M.Z.U. Rashid, M.I. Kamrul, and A. Islam. Understanding the Security Threats of Esoteric Subdomain Takeover and Prevention Scheme. In Proc. of ECCE ’19, pp. 1–4, 2019.

[13] M. Squarcina, M. Tempesta, L. Veronese, S. Calzavara, and M. Maffei. Can I Take Your Subdomain? Exploring Same-Site Attacks in the Modern Web. In Proc. of USENIX Security ’21, pp. 2917–2934, 2021.

[14] B. Laurie, A. Langley, and E. Kasper. Certificate Transparency. RFC 6962, IETF, 2013.

[16] WHATWG - Fetch Living Standard. https://fetch.spec.whatwg.org/#cors-protocol.

[17] D. Akhawe, F. Braun, F. Marier, and J. Weinberger. Subresource Integrity. REC-SRI-20160623, W3C, 2016.

[19] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 2008.

[23] Handshake. https://handshake.org.

[24] P. Hoffman and J. Schlyter. The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA. RFC 6698, IETF, 2012.