Design of Originator Profile

Shigeya Suzuki, Ph.D

Chair of Technology WG, Originator Profile CIP

Project Professor, Graduate school of Media and Governance, Keio University

2024/9/25 @ OP Breakout session at TPAC 2024

What OP provides for the Web

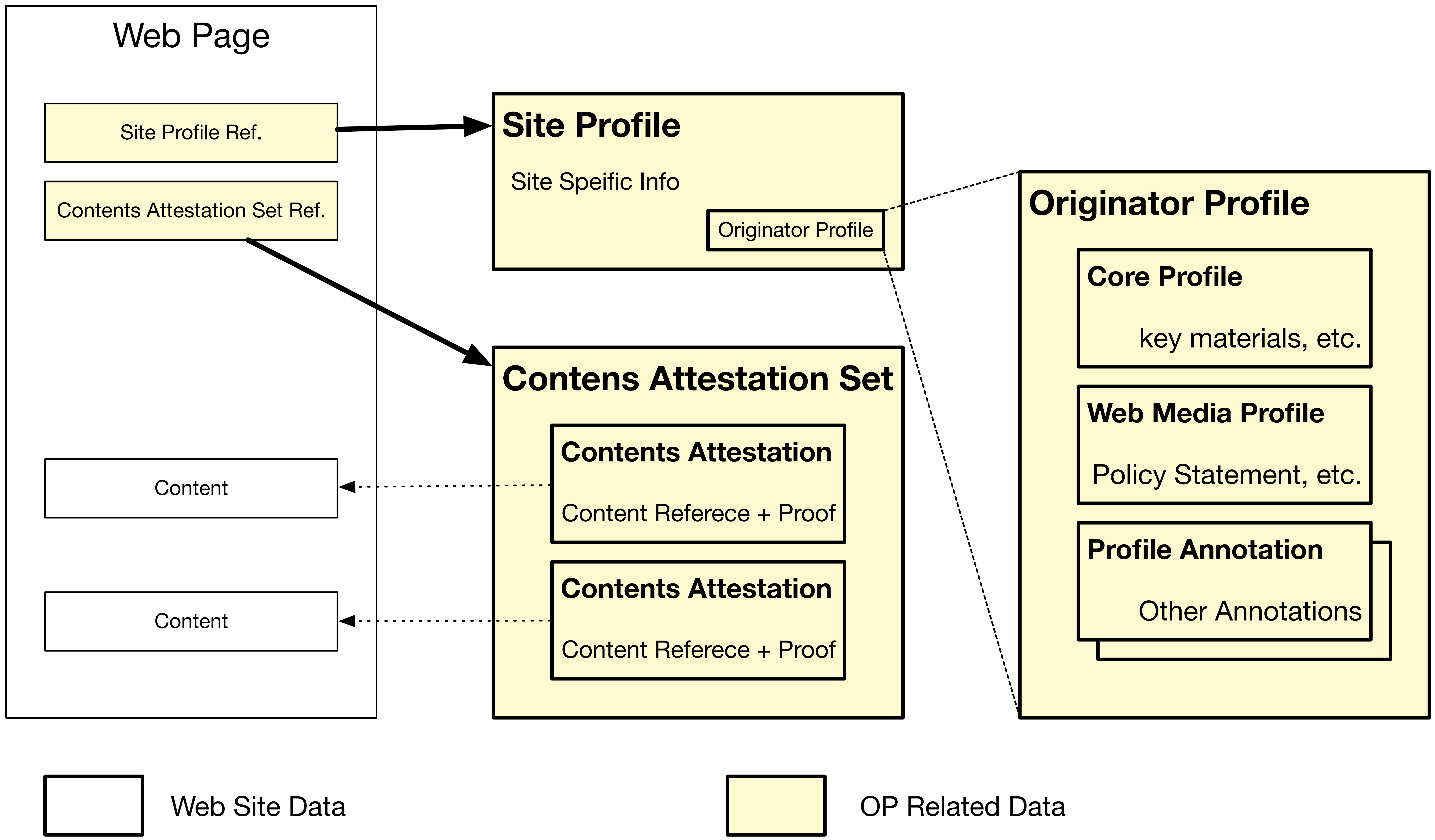
- Fragments of text or media (content) may accompanied with **Content Attestation**
  - **(Note: in the Video, it was introduced as DP (Document Profile))**
- The contents' Origin Identity as **Originator Profile (OP)**

Components

- Common Technology
  - Identity
  - Data Model
  - Presentation
- Baseline Governance Model

- Application Specific Implementation
  - Web Contents Authenticity

Data Model: Web Contents Authenticity

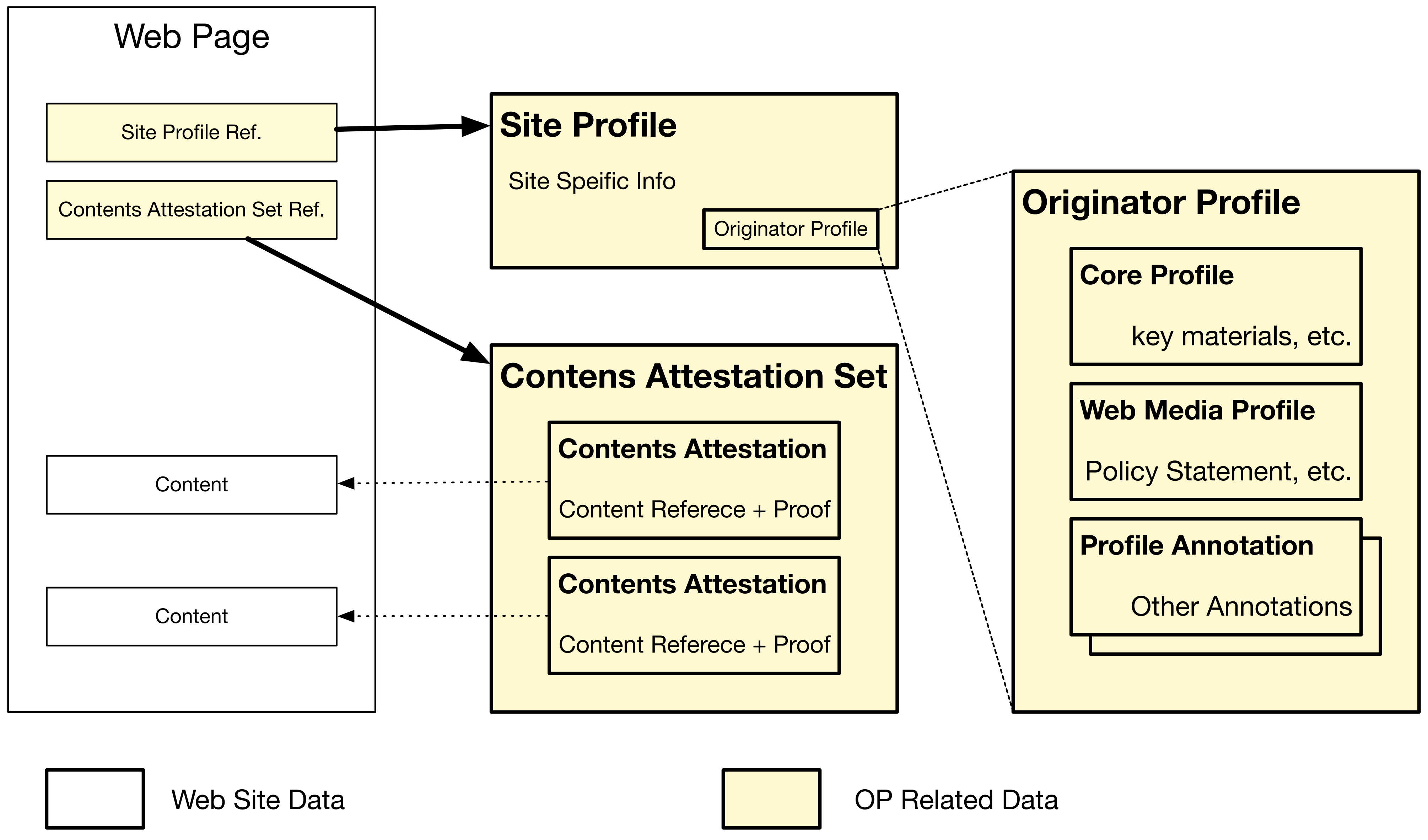


Data Model: Web Contents Authenticity

- **Originator Profile** consists of Core Profile, Web Media Profile (Web Media Specific) and one or more Profile Annotations, such as Proof for Existence of Organization

- Each of contents to be protected accompanied with **Contents Attestation** each of them includes reference into the web page, proof, and reference to Originator Profile

- Placement and delivery of each of information is highly flexible



Web Page

Site Profile Ref.

Contents Attestation Set Ref.

Content

Content

Site Profile

Site Speific Info

Originator Profile

Contens Attestation Set

Contents Attestation

Content Referece + Proof

Contents Attestation

Content Referece + Proof

Originator Profile

Core Profile

key materials, etc.

Web Media Profile

Policy Statement, etc.

Profile Annotation

Other Annotations

□ Web Site Data

▨ OP Related Data

Identity

- Originator Profile includes Human Readable, and Machine Processable information with source authenticity
- Application Specific (such as Web Media) Profile is separated for flexibility

- Originator Profile consists of
  - **Core Profile**: The key material the origin use — minimizing aims to potentially store in (or derived from) DNS RR
  - **Web Media Profile**: Profile specific to Web, such as the origin's policy statements, etc.
  - **Profile Annotations**: Additional information, potentially issued by third party,
    - Origin's information (country specific) with entity verification
    - Certifications
    - Memberships
    - Any kind of tagging

Presentation (implementation details)

- Currently implemented as a Browser Extension

- Extension only start working on pressing extension button

Baseline Governance Framework

- Profile Issuers for initial deployment
  - Core Profile, Application Specific Profile (Web Media Profile), and Organization Profile (includes existence verification) are issued from Originator Profile CIP only for OP launch
  - For Japanese newspapers, third party membership certification is provided from The Japan Newspapers Publishers and Editors Association
  - We will add other certifier for each of the use cases as needed
    - I,e., Japanese Government for Local Government Profiles

- We provide Baseline Governance Framework Design, but we don’t aim to be authority in the future

Chain of Trust and Machine Processing

- OP is designed to allow lightweight decision making as per Identity possible
    - “Profile Annotation” may be applied to Core Profile by anybody
    - The subject (owner of the Core profile) can decide which Profile Annotation to be paired with their web site
    - OP consumer can decide whether accept or reject an OP by:
        - Checking issuer of the Profiles are acceptable issuers
        - Using Profile’s data (including types, attributes)

- Examples:
    - Publisher may limit the contents to the page if the content’s origin’s Originator Profile contains specific type of certification from specific certifier (Certificate issuer)

Gaps OP fills

- Identity vs X.509 PKI
  - X.509 Does not provide scalability or flexibility wrt Governance
    - Usually policy applied to all of the members
    - Not reasonably operable for smaller group (community size scalability)

  - Scalability challenges (OCSP?)

Development Status

- Initial development completed, adjusting features

- Deployment Phase 1 : Limited number of Media outlets
  - Early CY2025
  - Missing features
    - Identity flexibility (incl. key rotation), more OP data placement flexibility

- Deployment Phase 2 : Outlet via aggregators, Digital Advertising
  - CY2025
  - Feature complete for static web sites

- Deployment Phase 3 : Local Government outlets
  - CY2025

…

Standardization and Discussions

- Data
  - SRI feature extension needed
  - Fragment Reference scheme

- Identity
  - Abstract model?
  - Potentially use in other applications if we design “Digital Identity for Machines” well
    - Simpler, Lightweight, easy to Machine Processable

- Presentation
  - Needs discussions on when to start process, when/how to show the result, how to alert verification failure, etc.
  - Potentially included as part of browser

- Governance Model

SRI for external resources and SRI extension (1)

- Content Attestation includes integrity (currently sha256) property of target contents (select HTML elements with CSS selectors and serialize them with outerHTML or textContent etc.) for HTML flow contents

- As for embedding content tags such as <img>, <audio>, <video> etc., we'll verify external resource files with integrity property of them. CA includes integrity property with same value as integrity property of those tags

- Current Problem/Limitations:
  - Current SRI spec and browser implementations don't support for them.
  - Current SRI spec don't support integrity for multiple resources with single tag.

```
e.g. <img src=“img200.png”   srcset=“img400.png 2x” ...>

     <video src=“video.mp4” poster=“poster.jpg” ...>
```

SRI for external resources and SRI extension (2)

- Our proposals for SRI extension will be:
  - Support SRI for additional external resources types (not only script and css)
  - Define integrity property for multiple resource with single tag.

```
e.g. <img src="img200.png" integrity="sha-256..."
                srcset="img400.png 2x" srcset-integrity="sha-256..." ...>

     <video src="video.mp4" integrity="sha-256..."
                poster="poster.jpg.png 2x" poster-integrity="sha-256..." ...>
```

- note: We currently not intend to sign target contents directly (not like signature-based SRI proposal, we intend to sing integrity property within the VC for better performance and cost.