Use of Name Redaction for Mass Devices

Tadahiko Ito (Secom)
Background

- draft-strad-trans-redaction-01
  - Name Relation was taken out of 6962-bis.(IETF97)
  - Expired (July 21, 2017)
  - Discussion was focusing on privacy
- My motivation
  - Some IoT devices might be outside the scope of “CT for web PKI”
  - We should have interoperability with “none-web PKI certificates”
    - Increase in IoT devices and scalability issue
    - security
  - Seems fine with same mechanisms as draft-strad-trans-redaction-01
We use server certificates for many devices

- Increase in Devices-to-Devices Communication is expected
  - one of the communication parties will use server certificate.

- Surveillance Cameras
  - We do not need a surveillance system for surveillance cameras
    - Need of TLS for confidentiality
  - Viewed / Connected by consumer devices (i.e. smartphone)
    - Want to tie to public root
  - Over the air firmware / certificate update
    - e.g.) issue one month certificate,
To make devices management easier

- Information for physical identification
  - Geometry information, model or lot number of Product
    - Sometime, people miss-install or miss-behave
  - Want to describe important information on the certificate, to manage the IoT devices

- Security
  - Above information is useful for
    - physical attack against devices
    - construct botnet
    - hiding them for security is “security through obscurity”? 
  - Attack surface may increase with CT
Do we need other mechanisms to deal with IoT devices?

- Current Mechanisms (draft-strad-trans-redaction-01)
  - Wild card
    - may not work with IoT devices at all
  - Use of name constraint intermediate
    - seems fit with my situation
  - Use of domain Label name redaction
    - Able to determine service provider / device vendor without showing identity of devices.

- Is it enough?
  - Do we have any better mechanisms?
<table>
<thead>
<tr>
<th></th>
<th>Plain method (Current CT)</th>
<th>Tec-Const Intermediate</th>
<th>Domain Label Redaction</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Monitor</strong></td>
<td>Can detect mississue</td>
<td>can not detect mississue</td>
<td>Can detect mississue</td>
</tr>
<tr>
<td><strong>Log Server</strong></td>
<td>Massive data</td>
<td>Not much difference</td>
<td>Massive Data</td>
</tr>
<tr>
<td><strong>Browser</strong></td>
<td>No change</td>
<td>implementation cost</td>
<td>High Implementation cost</td>
</tr>
<tr>
<td><strong>CA</strong></td>
<td>No change</td>
<td>Need constrained intermediate CAs</td>
<td>Implementation cost</td>
</tr>
<tr>
<td><strong>Service Provider / Device Vendor</strong></td>
<td>Can not put geo-information on cert.</td>
<td>Can put geo-information on cert.</td>
<td>Can put geo-information on cert.</td>
</tr>
</tbody>
</table>

- If it were enough, I want draft-strad-trans-redaction-01 back with security and scaleability.
- If we have any better mechanisms, I would like to explore that.