Public-key cryptography with mutual authentication for IoT platform

Jori Winderickx


**Introduction**

How to implement the IoT platform of ELL-i with IP-enabled security?

<table>
<thead>
<tr>
<th>Platform:</th>
<th>Objectives:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Service</td>
<td>Interoperable</td>
</tr>
<tr>
<td>Leaf node</td>
<td>Lightweight</td>
</tr>
<tr>
<td>Site Controller</td>
<td>Open source</td>
</tr>
</tbody>
</table>

**Methods**

Interoperable:
- Standards

Lightweight:
- Public-key algorithm
- Authentication process
- Libraries

Trust:
- Mutual authentication

**Results**

- DTLS
- X.509 certificate
- ECDSA_ECDH_AES_CCM_8
- DTLS interface for JavaScript
- WolfSSL

**Conclusion**

- Automatic integration
- Mutual authentication
- Interoperable
- Secure connection
- Open source

Promotoren / Copromotoren: Teemu Hakala
Prof. dr. Nele Mentens