

OAuth Native Apps and Device Posture

<draft-wdenniss-oauth-device-posture-01>

- Native apps: same code is distributed and used on a wide variety of devices.
- Today neither authorization servers nor resource servers learn about the hardware and software environment a specific OAuth client (app) is running in.
- OAuth is increasingly used for high assurance level use cases, such as payments, electronic signing, medical services.
- Getting this extra information provides valuable security signals.

Internet of Things

Hardware
Platform A

Hardware
Platform B

How to communicate information
about the hardware and software
components?

Server(s)

```
graph LR; A[Hardware Platform A] --> B[How to communicate information about the hardware and software components?]; B --> C[Server(s)];
```

The diagram illustrates the communication flow in an Internet of Things (IoT) system. On the left, there are two hardware platforms: 'Hardware Platform A' (represented by a blue rounded rectangle) and 'Hardware Platform B' (represented by an orange rounded rectangle). A large white arrow with a black outline points from these platforms towards the right. Inside this arrow is the text 'How to communicate information about the hardware and software components?'. The arrow points to a gray triangle on the right, which is labeled 'Server(s)'. This represents the data being sent from the hardware to the server for processing and storage.