Security for IoT
It all starts with trust!

**KEY PLAYERS**

4 super heroes fighting for Security in IoT against villain threats!!

- **“Super-DEVICE”**
  - Reliability
  - Hardware tailored for industry
  - On-device security: Encryption, IP protection

- **“Giant-ECO-SYSTEM”**
  - Authentication, trusted service management, data right management

- **“Wonder-DATA”**
  - Data privacy, encryption, authentication and identification

- **“Flash-NETWORK”**
  - Security at the Core

**FUNDAMENTALS**

- **Authentication / identification**
  Each device needs to be able to identify itself + prove its entitlement to access system

- **Confidentiality**
  Data transmitted must be encrypted effectively ensuring it is of no value to anyone stealing it

- **Integrity**
  Ensuring that what is sent is what is meant to be sent

- **Non repudiation**
  Incontrovertible proof of the validity and origin of all data transmitted

**KEY FIGURES TO KNOW ABOUT SECURITY IN IoT**

- **42%** believe security challenges represent the biggest inhibitor to IoT.
- **45%** say between 10%-40% of IoT data will be considered "sensitive".
- **45%** reckon wifi is the most challenging technology to secure.
- **37%** see platform standardisation issues as the biggest challenge.

*source: the IoT Outlook 2015, a report by Telecoms.com Intelligence*