EINDHOVEN OPEN DATA

WORK IN PROGRESS - v1.0

Smart Society Charter

IoT Architecture principles & guidelines

City of Eindhoven

In a Smart Society, digital online technologies become seamlessly integrated in the physical offline world, to improve people's lives and contribute to the development of the society. The most important thing in a Smart Society is that people experience the benefits of what the intensive co-evolution of digital and analogue, virtual and physical, online and offline will bring them.

With more and more technologies on the Internet of Things, and increasing volumes of data being collected, it is inevitable that IoT and data-driven services will have a serious impact on our lives. As a pioneer of the Smart Society, the City of Eindhoven is already facing up to imminent changes, and confronting the dilemmas that the new technologies bring with them. In order to safeguard public interest, stimulate innovation, foster a sustainable ecosystem of partners and encourage socially responsible business models, we have put together a few simple common principles to apply to an architecture of all current and emerging IoT initiatives across the city.

These principles are being developed in cooperation with commercial partners, start-ups and small enterprises, independent IoT developers, academic and research institutes, citizen-driven initiatives and other public organizations. We believe that these principles reflect our common values, contribute to the development of the city and improve the quality of life of its residents. We call on all IoT parties in Eindhoven, as well as our Dutch and international partners, to adopt, extend and reflect on these principles when building new or improving existing IoT and data infrastructures, platforms, services and applications. In a Smart Society, all participants should benefit from technology's achievements.

1 Privacy first

First and foremost, the privacy of the users and citizens should be guaranteed.

People should be given insight into the data that is collected and control over the way it is and will be used. Ethical aspects should be taken into account when extending practices into areas not addressed by current legislation.

2 Open data and interfaces

We facilitate innovation by making data publicly available and enabling access to IoT & data systems through open interfaces.

We stimulate new business models and emerging services that rely on generating added value, rather than exploiting licenses on data or exclusive rights on the infrastructure. We recommend making the infrastructure open on the lowest level and making raw data publicly available whenever this can be done without compromising the privacy and security of the citizens.

3 Embrace open standards

Wherever available, the IoT infrastructure, connectivity, platforms, devices and services should be built on open or broadly agreed de-facto standards.

Using established standards will facilitate evolution of infrastructure and services, sustain a competitive market and prevent vendor lock-in. Where standards are not yet available, maintaining openness and sharing best practices will help to lay a foundation for the future.

4 Share where possible

We expect all IoT and Data developments to provide well-defined, easily accessible stable interfaces for sharing and reusing existing assets.

Shared use of grids, sensor networks, connectivity and software components will lower the barriers for their adoption, increase connectivity and stimulate interoperability. The IoT & Data infrastructure should be available for re-use, as well as open to innovation and expansion.

5 Support modularity

We recommend adopting a modular architecture with well-defined open interfaces as the core of any IoT or data-driven development.

Modularity helps to ensure interoperability between platforms, services and applications and facilitates re-use and cooperation between partners.

6 Maintain security

The reliability of components, platforms, solutions and services must be constantly safeguarded.

Ensuring confidentiality, integrity and availability is vital to essential services and core parts of the infrastructure, which need to be safeguarded to the highest possible degree. In addition, all digital assets must be well-protected from attack, damage or unauthorized access.

7 Accept social responsibility

Providing new technologies and services, and collecting and combining data may result in unforeseen effects on society or individuals.

We cannot predict the future. We encourage experimentation, provided responsibility is taken for the consequences.

Data residing in the public space:

- Data residing in the public space (further on: data) belong to everyone. These data are an asset of the public. Data that are collected, generated or measured (for example by sensors that are placed in the public space) should be opened up in such way that everyone can make use of it for commercial and non-commercial purposes. While doing so, privacy and security aspects should be taken into consideration.
- Data may contain personal information. These data can therefore impact the private life of individuals. The rules specified in the Personal Data Protection Act are applicable here. These data may only be opened up after they have been processed (for example, by anonymization or aggregation) such that there are no privacy threats anymore.
- Data which do bring privacy or security risks along may only be used according to the privacy legislation. Storage and processing of these data should be performed according to the existing legislation.
- Data that do not contain personal information (anymore) should be placed in such way that everyone can access these data in an equal manner (for example, through an Open Data portal). We call this “opening up” the data. There should be no technical or juridical obstacles that limit, discriminate or block access to data.
- Data are always opened up free of charge, without unnecessary processing (as much as possible in a raw form) and according to the functional and technical requirements that are yet to be defined.
- A distinction is made with regard to personal data (such as an e-mail address or payment information) that are collected with full awareness and after an explicit consent of the individuals. Use of these data is defined by an agreement between the parties involved according to the rules of privacy legislation (such as an end user agreement).
- The city authorities always have an insight into which data are collected in the public space, independently of whether these data can or cannot be opened up.

- The city authorities keep an ongoing dialog with the parties that contribute to the development of data infrastructure in the city and strive to create earning opportunities and a fruitful economic climate.