PAS 185:2017

Smart Cities – Specification for establishing and implementing a security-minded approach

CPNI
Centre for the Protection of National Infrastructure

Department for Business, Energy & Industrial Strategy

bsi.

Publishing and copyright information

ISBN 978 0 580 96270 7

ICS 13.020.20

Publication history

First published November 2017

Contents

List of figures

Foreword

This PAS was sponsored by the Centre for the Protection of National Infrastructure (CPNI). Its development was facilitated by BSI Standards Limited and it was published under licence from The British Standards Institution. It came into effect on 30 November 2017.

Acknowledgement is given to the technical authors Alexandra Luck and Hugh Boyes, and to the following organizations that were involved in the development of this PAS as members of the steering group:

- A Luck Associates
- Arup
- BIM Task Group
- Bodvoc Ltd
- City of Bradford, Metropolitan District Council
- Bristol City Council
- Cities Standards Institute
- Centre for the Protection of National Infrastructure (CPNI)
- Department for Transport
- Digital Catapult
- FlyingBinary
- Future Cities Catapult
- Institute of Asset Management
- IoT Security Foundation
- National Cyber Security Centre (NCSC)
- Peterborough City Council
- Trustworthy Software Foundation
- Turner & Townsend
- University of Cambridge, Centre for Smart Infrastructure and Construction
- Co-opted member

Acknowledgement is also given to the members of a wider review panel who were consulted in the development of this PAS.

The PAS process enables a specification to be rapidly developed in order to fulfil an immediate need in industry. A PAS can be considered for further development as a British Standard, or constitute part of the UK input into the development of a European or international Standard.

Relationship with other publications

This PAS is issued as part of a suite of BSI publications related to smart cities:

- PAS 180, *Smart cities – Vocabulary* defines terms for smart cities, including smart cities concepts, across different infrastructure and systems elements and used across all service delivery channels;
- PAS 181, *Smart city framework – Guide to establishing strategies for smart cities and communities* gives guidance on a good practice framework for decision-makers in smart cities and communities (from the public, private and voluntary sectors) to develop, agree and deliver smart city strategies that can transition their city's ability to meet future challenges and deliver future aspirations;

- ISO 30182, *Smart city concept model – Guide to establishing a model for data interoperability* provides a framework that can normalize and classify information from many sources so that data sets can be discovered and combined to gain a better picture of the needs and behaviours of a city's citizens (residents and businesses);
- PAS 183, *Smart cities – Guide to establishing a decision-making framework for sharing data and information services*, gives guidance for decision-makers from the public, private and third sectors on establishing a framework which can support the sharing of city data and the creation of interoperable information services;
- PAS 184, *Smart cities – Developing project proposals for delivering smart city solutions – Guide*, provides guidance, illustrated with case studies, on how good practice described in other BSI smart city publications can be applied when developing an individual project proposal within the broader smart city programme;
- PD 8100, *Smart cities overview – Guide* gives guidance on how to adopt and implement smart city products and services in order to facilitate the rapid development of an effective smart city;
- PD 8101, *Smart cities – Guide to the role of the planning and development process* gives guidance on how the planning and implementation of development and infrastructure projects can equip cities to benefit from the potential of smart technologies and approaches.

Use of this document

It has been assumed in the preparation of this PAS that the execution of its provisions will be entrusted to appropriately qualified and experienced people, for whose use it has been produced.

Presentational conventions

The provisions of this PAS are presented in roman (i.e. upright) type. Its requirements are expressed in sentences in which the principal auxiliary verb is "shall".

Commentary, explanation and general informative material is presented in italic type, and does not constitute a normative element.

Where words have alternative spellings, the preferred spelling of the Shorter Oxford English Dictionary is used (e.g. "organization" rather than "organisation").

Where URLs for websites and webpages have been cited, they aim to provide ease of reference for the PAS user and are correct at the time of publication. The location of a webpage or website, or its contents cannot be guaranteed.

Information about this document

Copyright is claimed on Figure 4. The copyright holder is Hugh Boyes.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a PAS cannot confer immunity from legal obligations.

Particular attention is drawn to the following specific regulations:

- Computer Misuse Act 1990 [1]
- Data Protection Act 1998 [2]
- Environmental Information Regulations 2004 [3]
- Freedom of Information Act 2000 [4]
- Freedom of Information (Scotland) Act 2002 [5]
- General Data Protection Regulation (GDPR) (Directive 95/46/EC) [6]
- Investigatory Powers Act 2016 [7]
- Measures for a high common level of security of network and information systems across the Union (Directive EU 2016/1148) [8]
- Official Secrets Act 1989 [9]
- Planning and Compulsory Purchase Act 2004 [10]
- Privacy and Electronic Communications Regulations 2003 [11]
- Public Records Act 1958 [12]
- Public Records Act 1967 [13]
- Re-use of Public Sector Information Regulations 2005 [14]

0 Introduction

PAS 185 is a companion document to:

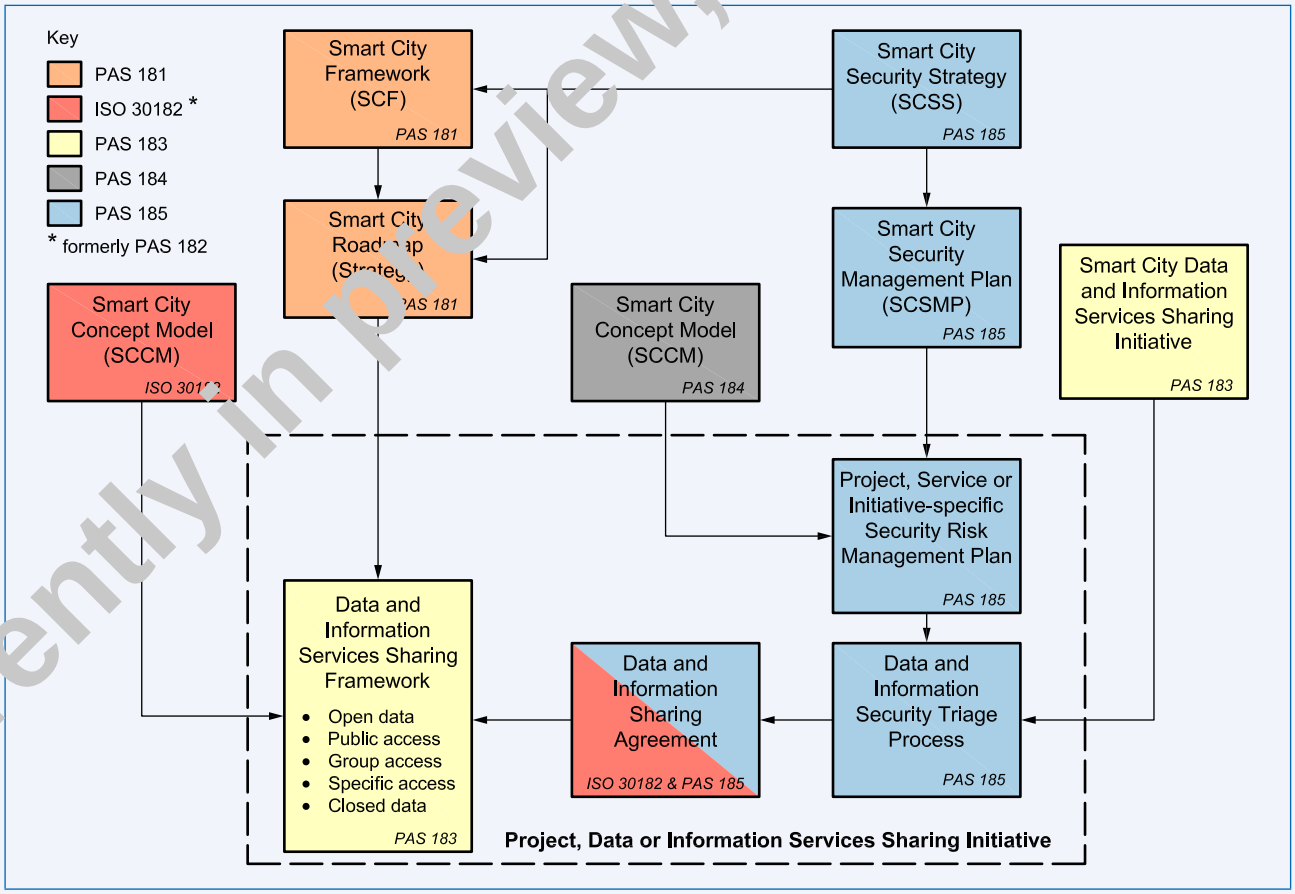
- PAS 180, *Smart cities – Vocabulary*;
- PAS 181, *Smart city framework – Guide to establishing strategies for smart cities and communities*;
- ISO 30182, *Smart city concept model – Guide to establishing a model for data interoperability*;
- PAS 183, *Smart cities – Guide to establishing a decision-making framework for sharing data and information services*;
- PAS 184, *Smart cities – Developing project proposals for delivering smart city solutions – Guide*;
- PD 8100, *Smart cities overview – Guide* gives guidance on how to adopt and implement smart city products and services in order to facilitate the rapid development of an effective smart city; and
- PD 8101, *Smart cities – Guide to the role of the planning and development process* gives guidance on how the planning and implementation of development and infrastructure projects can equip cities to benefit from the potential of smart technologies and approaches.

It makes reference to the definitions and concepts contained within these publications and complements them by showing how a city-wide, strategic-level, security-minded approach can be applied alongside the development of a smart city framework, a smart city strategy and roadmap, frameworks for sharing data and information services, and project and data and/or information services sharing initiatives.

The relationship of PAS 185 to the key concepts set out in each of these companion documents is shown in Figure 1.

A security-minded approach comprises the routine application of appropriate and proportionate security measures to deter and/or disrupt hostile, malicious, fraudulent and criminal behaviours or activities. Further, it considers security holistically, looking at personnel, physical, cyber and cross-cutting issues and solutions.

Figure 1 – The integration of the security-minded approach



PAS 185 is also consistent with the approach set out in PAS 1192-5, which relates to the security-minded management of building information modelling (BIM), digital built environments and smart asset management. This consistency allows the appropriate sharing and disclosure of geospatial, dynamic and asset information in order to support service planning, development and delivery of assets and services in smart cities.

Where a service applies to multiple assets and/or data and information is shared or processed by other city organizations, the security-minded approach set out in PAS 185 can be applied. However, where a service relates solely to a built asset and the asset data and information is not shared with, or processed by, another city organization, a number of requirements contained within this PAS are not applicable. In these cases, where the asset is deemed sensitive, the security-minded approach set out in PAS 1192-5 can be implemented.

The underlying premise of smart cities is that greater availability of data and information, integration of services and systems, and outcome-based contracting can:

a) increase the capacity, efficiency, reliability and resilience, and thereby availability, of existing assets to enable enhanced service provision for its citizens; and

b) improve efficiency in design and delivery of new built assets through a better understanding of whole-life performance of those built assets already in place.

A key purpose of a smart city is to join up specific vertical sectors (e.g. utilities, transport, health, etc.) across organizational boundaries into a whole-city approach for the creation, delivery and use of city spaces and services. These changes should enable the city to:

1) take better account of the needs of current and future citizens;

2) integrate physical and digital planning;

3) more efficiently and sustainably identify, anticipate and respond to emerging challenges, including emergency situations; and

4) increase the capacity for service delivery and innovation which in turn has the capability to drive efficiencies and effectiveness.

Advancements in digital engineering, information and communication technologies are significant enablers of these changes. However, increased use of, and dependence on, these technologies, especially when coupled with much wider sharing and use of city data and information, and new service delivery models, also creates significant vulnerabilities and associated security issues. The threat actors associated with: organized crime; unauthorized acquisition of personal data, intellectual property and commercially sensitive data or information; terrorism; and malicious acts including sabotage, which disrupt or corrupt data/information and/or systems, might seek to make use of these vulnerabilities in order to compromise the value, longevity and ongoing use of a city's built assets and services, as well as the safety and security of a city's citizens.

The security-minded approach developed within a smart city therefore differs from any security-minded policies and processes which might already be in place within an individual local authority or other service delivery organization that needs to respond to the new or enhanced vulnerabilities created by changes to existing ways of working. These vulnerabilities include:

i) the increase in volume of data and information being generated, collected, utilized and stored, including personal data, intellectual property and commercially sensitive data and information;

ii) greater sharing and dissemination of data and information within and across organizations with various existing contractual arrangements in place;

iii) the potential aggregation of data and information from a wider range of sources; and

iv) potential differing organizational priorities, governance arrangements, policies and processes, security understanding and concerns, and risk appetite.

However, it is essential that the city-specific, security-minded approach adopted is appropriate and proportionate to the risks and does not prevent delivery of the city's aims. In addition, individual organizational security-minded policies and processes should, where applicable, support and complement this wider approach.

If the smart city is to gain, and maintain, the trust of its citizens it needs to be capable of responding to increasing citizen awareness and potential concerns about how their personal data is being used, and put in place mechanisms to prevent that trust potentially being abused. This need is reflected in European Union

(EU) by the tightening of data protection regulations in the development of the General Data Protection Regulation (GDPR) [6]. These regulations align with the Data Protection Act 1998 (DPA) [2] but also contain some new elements and significant enhancements. GDPR [6] will be enforceable in the UK from 25 May 2018. However, the UK and EU member states retain the ability to introduce national level derogations where these are required for specific purposes. Therefore, the specifics of how GDPR [6] will be implemented within the UK are not certain at the time of publication.

While the PAS is specifically written for smart city decision-makers and smart city data officers, whether from the public, private or third sectors, it might also be of relevance to those who are interested in utilizing data and information to deliver smart city objectives effectively.

1 Scope

This PAS specifies requirements for establishing a framework for the security-minded management of the city, including its associated assets, including data and information, and services.

It outlines methods for identifying security threats to a smart city, including those that might also affect the people who live, work in, trade from, or visit it. It also sets out parameters for mitigating other adversities on security systems.

It covers the use of trustworthiness and security controls applicable to the smart city framework (SCF) (see PAS 181), smart city concept model (SCCM) (see ISO 30182) and data framework used for sharing data and information services (see PAS 183).

The security-minded approach specified in this PAS covers all aspects of security relating to smart cities, including:

- governance;
- personnel;
- citizens;
- organizations;
- process; and
- physical security.

The approach also covers aspects of the environment of the smart city, including:

- scale;
- organizational complexity;
- complex service delivery and ownership of smart city infrastructure;
- response to incidents, events, and changing risk levels; and
- extent of autonomy.

This PAS covers technological aspects relating to the secure delivery of services, including:

- safety;
- authenticity;
- availability (including reliability);
- confidentiality;
- integrity;
- possession;
- resilience; and
- utility.

***NOTE** Definitions of these terms are given in Clause **3**.*

The framework specified in this PAS enables the development of an overall security strategy for the handling, management and sharing of data and information that can be used to inform and guide the development and delivery of smart city projects and subsequent operation, delivery, evolution and disposal of assets and services.

This framework can be used to create and cultivate an appropriate, risk-based safety and security mindset and culture across the many organizations, services and individuals which use shared, disclosed and derived data, and includes the need to monitor and audit compliance.

This PAS is for use by decision-makers in smart cities from the public, private and third sectors and smart city data officers. It might also be of relevance to those who are interested in utilizing data and information to effectively deliver smart city objectives.

***NOTE** PAS 185 is consistent with the approach set out in PAS 1192-5 regarding the security-minded management of building information modelling, digital built environments and smart asset management. This consistency is important as it allows appropriate, sharing or disclosure of geospatial, dynamic and asset information in support of service planning, development and delivery in smart cities.*