

# bsi.



## BSI Digital and Connected

Testing and certification solutions  
for a smarter, more secure world



# Build trust in your connected devices and software products

In our increasingly digital world, we rely on connected devices more than ever before. From smartphones to smart home appliances, these devices provide convenience and efficiency that have transformed the way we live and work. However, with the rise of connected devices, there has also been a growing concern over security and privacy. As we entrust more and more of our personal information to these devices, it becomes crucial to establish trust in their ability to protect that information.

In this document, we will explore BSI testing and certification solutions to build trust in your connected devices and software solutions to ensure a safe online environment and compliance with the upcoming IoT product cybersecurity legislation.

## BSI Digital and Connected testing and certification solutions – designed to build digital trust

At BSI, we focus on delivering testing and certification services underpinned by quality, safety, reliability, and trust. As a global organization, we have the scale and reach to support any size of organization and in our dedicated state-of-the-art IoT laboratory, our experts provide fast and effective testing for a wide range of IoT products.

BSI has a world-class cybersecurity capability recognized by UKAS accreditation, CREST global accreditation, National Cyber Security Centre, and IoT Security Foundation combined with decades of experience in product assurance and testing. We help you embed trust and confidence in your product, providing independent assurance of their safety and security.



National Cyber Security Centre

### BSI covers the following services and areas:

Cybersecurity certification for your organization

Cybersecurity testing and certification of products and devices

Web and mobile application testing and certification

Digital identity, electronic identification, and trust services



# Cybersecurity certification for your organization

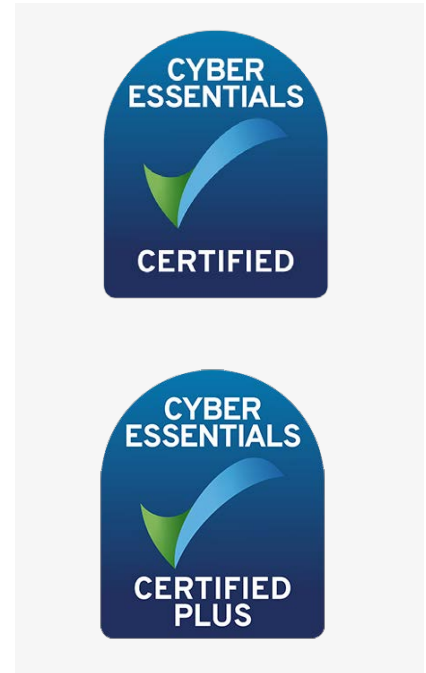
## Cyber Essentials

Cyber Essentials is an effective, UK Government-backed scheme that helps you protect your organization against a whole range of the most common cyber-attacks focusing on the following key areas: secure configuration, boundary firewalls and interned gateways, access control and administrative privilege management, and malware protection.

The Cyber Essentials scheme requires the completion of a self-assessment questionnaire.

## Cyber Essentials Plus

Cyber Essentials Plus certification is based on the same principles as Cyber Essentials along with a technical audit performed by a regulated auditor.



# Cybersecurity testing and certification of products and devices

## Cybersecurity for Consumer IoT devices according to ETSI EN 303 645 and ETSI TS 103 701

ETSI EN 303 645 is the first global cybersecurity standard for consumer IoT products. The standard brings together widely considered good practices in security for Internet-connected consumer devices in a set of high-level outcome-focused provisions.

The standard comprises 33 mandatory provisions and 35 recommendations, across 14 areas. These areas and provisions form the basis of developing product cybersecurity legislation around the world. Beyond any legislative requirements, manufacturers can choose to apply and have their products tested and certified against any subset of the provisions, or all applicable provisions, according to your product cybersecurity needs.

BSI offers UKAS-accredited third-party testing and evaluation of ETSI EN 303 645 provisions in accordance with ETSI TS 103 701 and the issue of certificates of conformity to limited or full requirements of ETSI EN 303 645

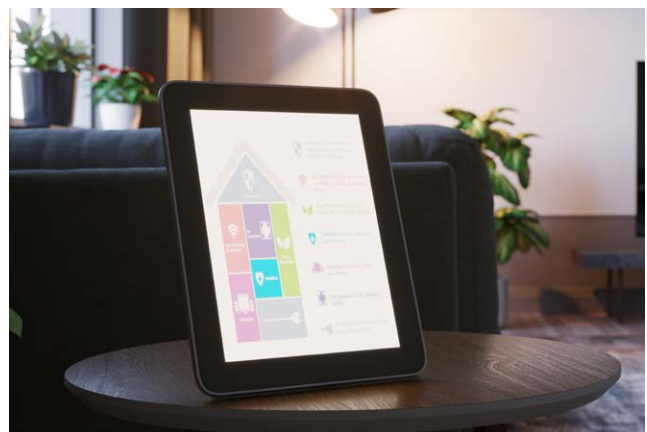
---

## UK Product Security and Telecommunication Infrastructure (PSTI) testing services and Certification of Conformity

On 6 December 2022, the UK Government passed a law on the Product Security and Telecommunication Act, also called the PSTI Bill. The new legislation will come into force on 29 April 2024.

The new law includes measures that will introduce a series of improved and relevant security protections to tackle ongoing threats of cybercrime.

The PSTI legislation covers connected safety-relevant products such as smoke detectors, fire detector and door locks; connected home automation devices, smart doorbells, and alarm systems; IoT-based stations and hubs to which multiple devices connect; smart home assist, smartphones, connected cameras (IP and CCTV),



wearables, connected fridges, washers, freezers, coffee machines, and other similar products.

BSI offers independent third-party testing against the different security provisions and certification of conformity stating if the product complies with the PSTI regulation.



## **RED Delegated Act Cybersecurity pre-testing services**

The European Commission (EC) has taken measures to strengthen the cybersecurity of wireless devices and products available in the European Union (EU) by adopting a Delegated Act under the 2014/53/EU Radio Equipment Directive (RED). The Delegated Act will enter into force on 1 August 2025.

The new RED Delegated Act aims to address cybersecurity testing of IoT devices before being placed onto the EU market. While harmonized testing standards for RED cybersecurity are still under development, by following the leading baseline ETSI EN 303 645 standard, you can ensure that your products meet the highest level of security and privacy for IoT devices. This standard is widely recognized and adopted by

regulators and industry stakeholders around the world. By complying with this standard, you can demonstrate your commitment to best practices and gain a global competitive advantage.

The measures cover wireless and IoT devices such as mobile phones, tablets, and other products capable of communicating over the internet; toys and childcare equipment such as baby monitors; and a range of wearable equipment such as smart watches, or fitness trackers.



## BSI IoT Kitemark™ certification

The IoT Kitemark certification scheme delivers trust, through the conduction of rigorous and independent tests covering functionality, interoperability, and security.

The scheme is not only a one-time verification, as it also incorporates an ongoing assurance, per its annual factory assessment requirements, which include assessments against all relevant scheme requirements related to all protocols associated with the product, and a review of the quality management system in place.

On top of that, it also includes rigorous functional testing for the physical and digital devices including full coverage against ETSI 303 645 / ETSI TS 103 701 and, finally, it also involves in-depth testing for any mobile and web application used to interact with the IoT product according to the well-known OWASP industry test standards.

Both testing activities for the hardware and software pieces are also performed on an ongoing basis to demonstrate continuous compliance with the latest security standards.

Robust and internationally recognized, the BSI Kitemark can help enhance a manufacturer's reputation and boost customer confidence.

In today's digital world, consumers face many challenges when choosing products that meet their needs and expectations. One of the most important factors is data security, which can have serious consequences if compromised.

That is why we created a tailored certification program that evaluates and verifies the data security standards of various products, from smartphones to smart home devices. Our certification program provides end consumers with a quick and straightforward way of identifying which products they can trust to not only perform as expected but also keep their data secure. By looking for our seal of approval, consumers can shop with confidence and peace of mind.

### The benefits of Kitemark certification

Achieving BSI Kitemark certification can help you to:

- **Increase your brand resilience** against the latest cybersecurity threats
- **Increase your customer base** and customer satisfaction
- **Provide end consumers with a quick and effortless way of identifying which products** they can trust to not only perform as expected, but also keep their data secure
- **Gain competitive advantage**



Application

Type Testing

Initial Factory Assessment

Continually Reflecting change  
Standards/Accidents/Regulations  
Technology/ Market expectations

## BSI IoT Kitemark for IoT devices

BSI IoT Kitemark certification scheme has been carefully developed based on the most relevant global and well-known security standards providing continual assurance and covering product supply chain and life cycle.

Our BSI IoT Kitemark is based on the following security standards and security recommendations principles:

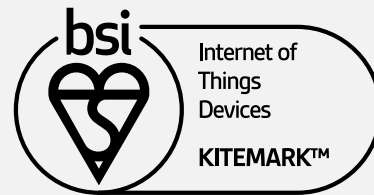
- **ETSI EN 303 645 / ETSI TS 103 701** for hardware-connected devices
- **ASVS and MASVS** for Digital applications and IoT-interfacing applications

We know the destination of quality and cyber security is a moving target, which is why our Kitemark certification includes continual assurance to make sure our clients are never out of step with industry standards.

BSI IoT Kitemark certification scheme proves that a product has been tested for functionality, interoperability, and security.

The BSI IoT Kitemark offers three levels of certification for IoT devices.

- Residential products used in a residential environment
- Commercial products used in a commercial environment
- Enhanced residential or commercial products for high-value/high-risk applications



## Cryptographic module security Certification of Conformity against ISO 19790

A cryptographic module is a set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) and is contained within a cryptographic boundary.

ISO / IEC 19790 with associated testing methodology standards ISO / IEC 24759 caters to varying degrees of data sensitivity by setting out four security levels for cryptographic modules – ranging from, for example, low-value administrative data to classified government information. The four security levels also account for different application environments

ranging, for example, from removable media in an unprotected location to a highly guarded data centre.

By creating consistency across industries and regions, ISO / IEC 19790 enables quicker delivery of secure, innovative, and transformative digital products to the global market and increases trust in connected products and smart solutions.

BSI is helping cryptographic module manufacturers to achieve Certificate of Conformity against ISO 19790 standard for their products.



### Smart EV charging regulations

From 30 June 2022, all-electric vehicle (EV charging) points sold and installed for private use must comply with the Electric Vehicles (Smart Charge Points) Regulations 2021.

The requirements are based on smart functionality, electricity supplier interoperability, off-peak charging, randomized delayed charging, continued charging, safety provisions, measuring systems, and security.

BSI has the required testing and certification experience to be the right partner for these legal regulations for all EV charger point manufacturers intending to sell their devices in Great Britain





## Web and mobile testing and certification

Mobile, web applications and software programs are designed to run on different platforms and devices, allowing users to perform various tasks -accessing information, enabling transaction handling, or even financial services. However, with new technological developments, both users' and businesses face a whole array of new risks that need to be addressed to protect users personal and financial data as well as brand reputation.

To address these challenges in an evolving market, BSI offers its clients tailored testing and certification to address the latest cyber threats and vulnerabilities. Our Secure Digital Applications Kitemark schemes are based on the industry-established standards and include requirements of **OWASP** (The Open Web Application Security Project):

- **ASVS** (The Application Security Verification Standard) for web applications
- **MASVS** (The Mobile Application Security Verification Standard) for mobile applications

The level of testing is dependent on the risk associated with the functionality and type of data stored and processed. These are:



# Digital identity, electronic identification, and trust services

## UK Digital Identity and Attributes Trust Framework (UK DIATF)

The UK Digital Identity and Attributes Trust Framework (UK DIATF) is a set of standards and best practices for organizations to follow if they want to provide secure and trustworthy digital identity and/or attribute solutions for a wide variety of applications safely and consistently.

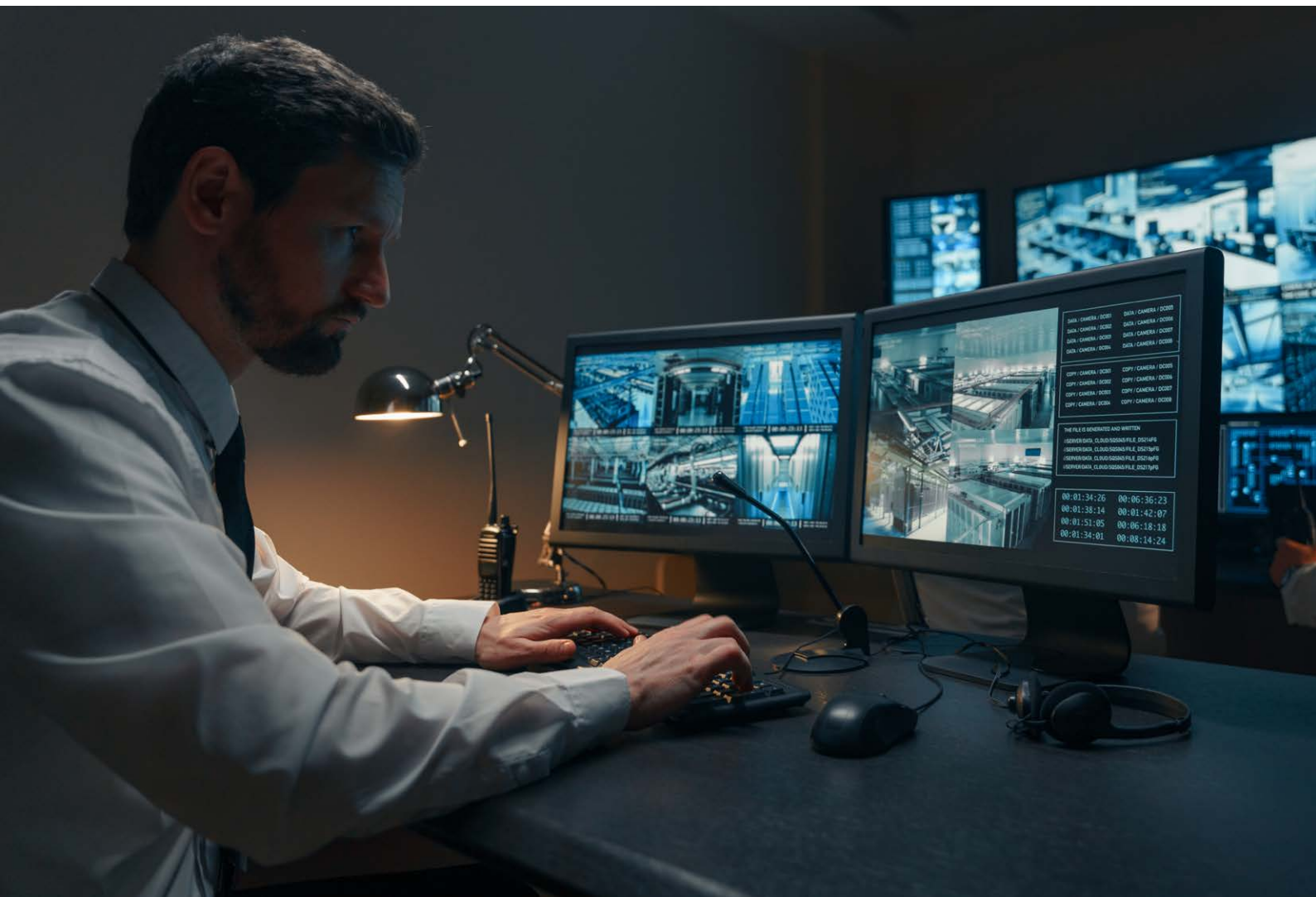
The purpose of the framework is to make it easier and more secure for people to use services that enable them to prove who they are or information about themselves.

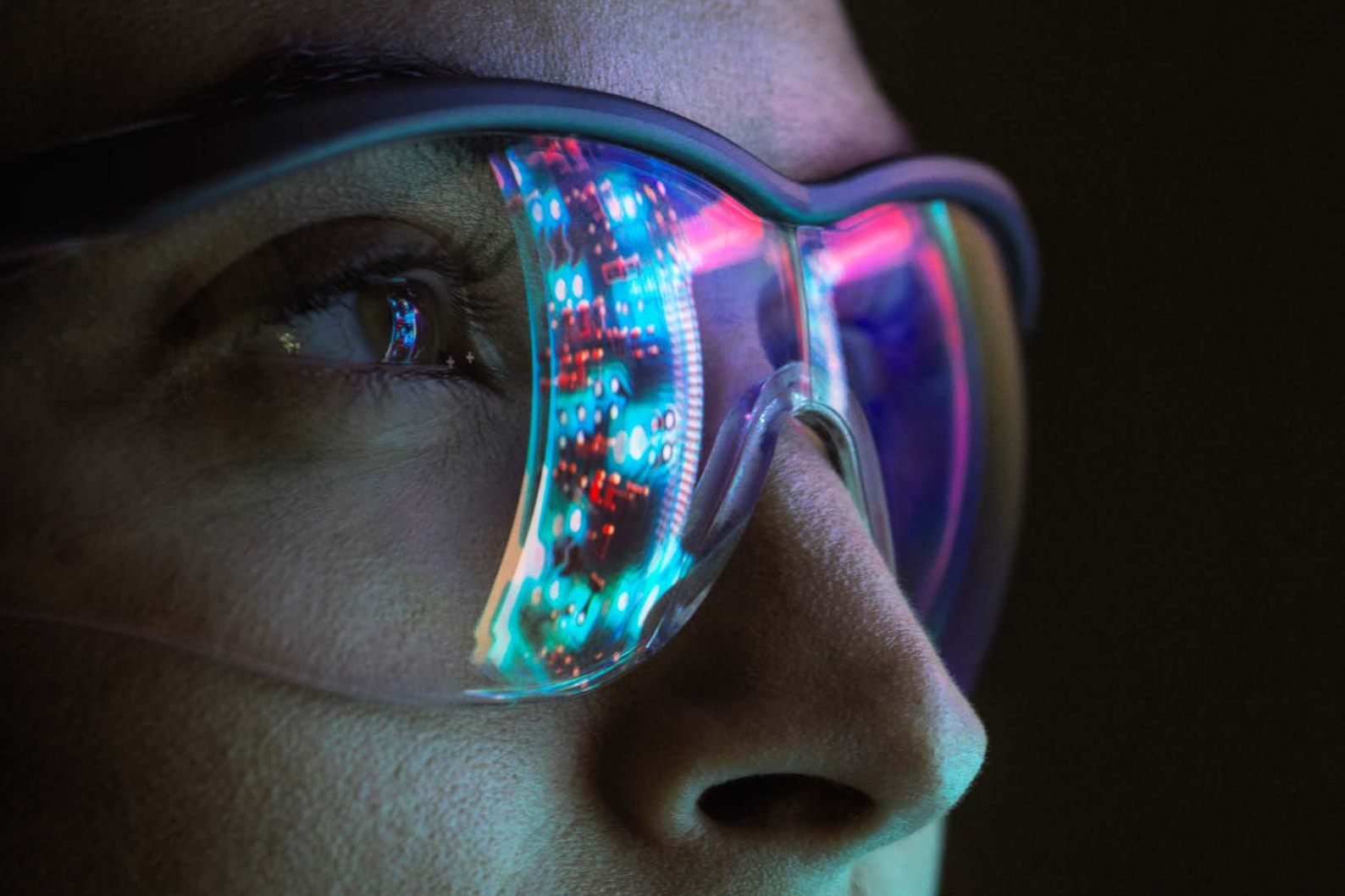
This is a key priority for the UK Government to enable innovation, and competition and provide transparency.

To achieve this, the trust framework is expected to require the service providers to become independently certified against the set of prescribed rules in the UKDIATF.

The UK DIATF is being piloted on specific applications (schemes) including:

- **Disclosure and Baring Service (DBS) digital vetting** (certification required)
- **Home office Right to Work** (certification encouraged)
- **Right to Rent** (certification encouraged)





## eIDAS and UK eIDAS

The eIDAS certification refers to the certification framework established by the European Union's Electronic Identification, Authentication, and Trust Services (eIDAS) Regulations. eIDAS is a regulation that sets standards for electronic identification and trust services in the EU.

BSI is a Conformity Assessment Body (CAB) ISO 17065 to carry out conformity assessments following the relevant ETSI standards and in accordance with the eIDAS regulation 910/2014. BSI is also the only CAB ISO 17065 accredited for the UK eIDAS regulation.



# eIDAS

The eIDAS Regulation, which came into effect on 1 July 2016, aims to establish a framework that allows for seamless cross-border recognition and acceptance of electronic identification and trust services across EU member states. It promotes the use of electronic identification (eID) and trust services, such as electronic signatures, electronic seals, electronic time stamps, and electronic registered delivery services.

The UK eIDAS Regulations are an amendment from the EU eIDAS Regulation and retain many aspects of the EU Regulation but are tailored for use within the UK. BSI Assurance is currently the only Conformity Assessment Body (CAB) in the UK for the eIDAS services accredited by UKAS.



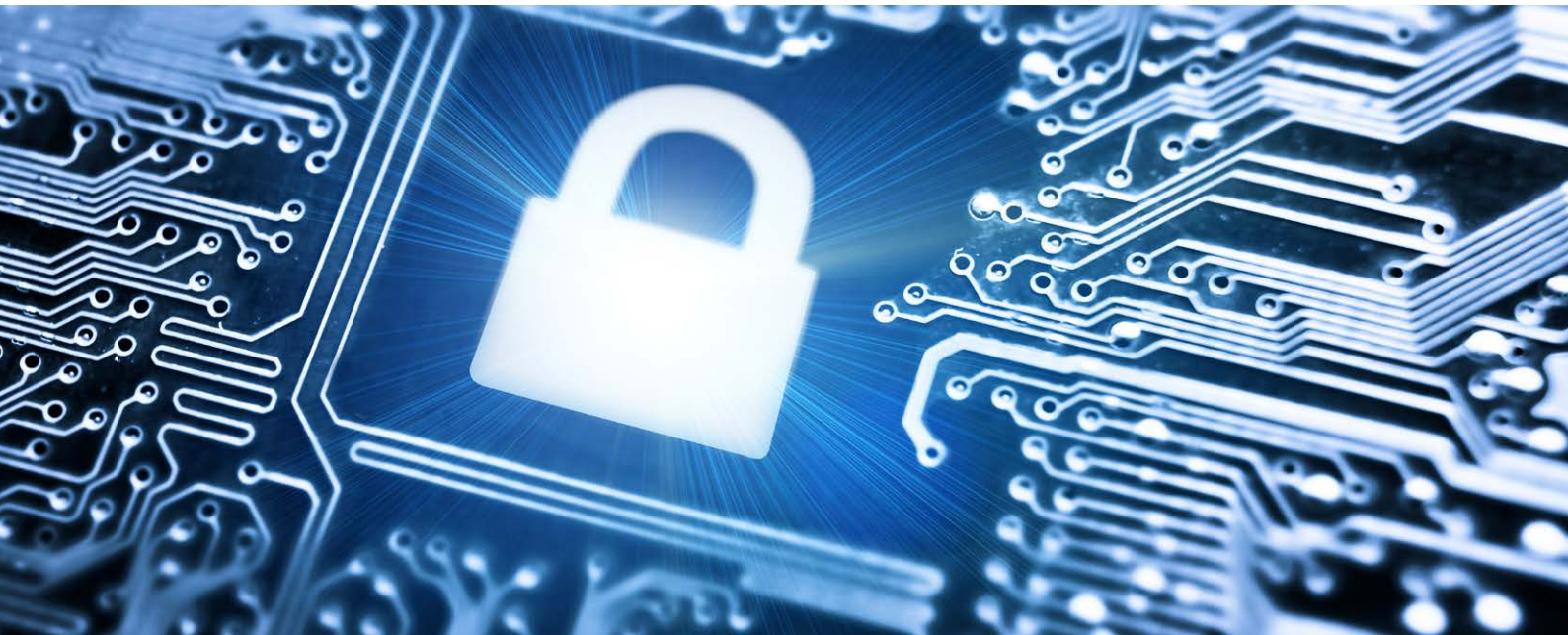
# About BSI



BSI works as a trusted, independent convenor of communities to shape, share, embed, and support innovation in IoT and the safe and reliable use of 'smart' applications, data, and devices. Through our community of IoT experts and organizations, BSI is at the forefront of shaping new opportunities and creating industry-led best practices in IoT. That's why we're best placed to help you embed trust and confidence in your products.

Working with over 84,000 clients across 193 countries, BSI is a truly international business with skills and experience across a number of sectors including automotive, aerospace, built environment, food, and healthcare. Through its expertise in Standards Development and Knowledge Solutions, Assurance, and Professional Services, BSI improves business performance to help clients grow sustainably, manage risk, and ultimately be more resilient.

**BSI: Inspiring trust for a more resilient world.**



**bsi.**

Get in touch today and find out more

Call: **+44 (0)345 0765 606**

Email: **[product.certification@bsigroup.com](mailto:product.certification@bsigroup.com)**

Visit: **[bsigroup.com/iot](https://bsigroup.com/iot)**

