WHITE PAPER

Contact Information

Brian Bishop
DATA PERFORMANCE CONSULTANCY & OCF PRESIDENT
brian.bishop@dpc-ltd.com

OCF Secretariat
staff@openconnectivity.org

OPEN CONNECTIVITY FOUNDATION®

OPEN CONNECTIVITY FOUNDATION®

Enabling Secure Communications in Smart Cities & Government Infrastructure

OCF'S ISO/IEC STANDARD ENABLES SECURE IOT COMMUNICATION OVER INTERNET PROTOCOL (IP), OFFERING A HOLISTIC APPROACH TO THE MANAGEMENT & OPTIMIZATION OF URBAN INFRASTRUCTURE

March 6, 2023

Market context

"While efforts to address cyber threats targeting ICT systems are generally well established in many organizations, the issue of managing threats targeting operational technology (OT) has only recently become a priority."[1] – OCF Member, TÜV SÜD

"New standards are required to support this greater software and hardware modularity, in order to avoid duplication, reduce development times and maintenance costs, and facilitate data sharing." – Robotics Growth Partnership

Deploying proprietary systems do not adequately meet the emerging challenges of developing smart city infrastructure such as the need for efficient data processing and analytics, agility, flexibility, privacy and coordination between the public and private sector.[2] The OCF specifications meet these challenges and allow for the development of open, interoperable smart cities. A recent UK Cyberphysical Infrastructure report brought the need for OCF specifications to light, highlighting the need for "Common standards for hardware and software components to support interoperability and the creation of pre-competitive building blocks to accelerate innovation".

With most systems yet to transition to IP based connectivity, data cannot be carried over regular ethernet networks. This means elements of connectivity such as Wi-Fi networks are managed by Information Technology (I.T)[3] professionals, while management of essential functions (lights, heating etc.) are managed by Operational Technology (O.T.)[4] professionals.

The emergence of IP based technology is resulting in crossover between IT and O.T. professionals. For the benefits of IP based technology to be realized, O.T and I.T. professionals must collaborate to ensure this skills gap is closed.

The OCF standard allows for the bridge between O.T. & I.T. to happen. The OCF specification sits between these two worlds, and can be used to aid education and implementation of security-based ISO/IEC protocols.

[1] https://www.tuvsud.com/en-gb/resource-centre/white-papers/iec-62443-industrial-security
[2] https://statetechmagazine.com/article/2018/12/6-challenges-smart-cities-face-and-how-overcome-them

[3] "IT" is the common term for the entire spectrum of technologies for information processing, including software, hardware, communications technologies and related services. In general, IT does not include embedded technologies that do not generate data for enterprise use." - https://www.gartner.com/en/information-technology/glossary/it-information-technology

[4] "Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise". - https://www.gartner.com/it-glossary/operational-technology-ot/

Introduction to OCF

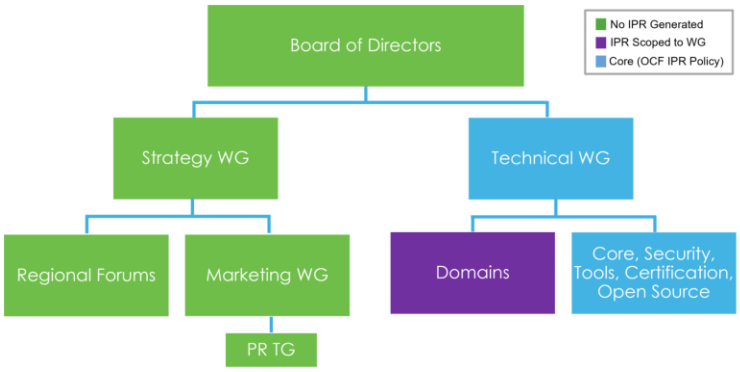
"OCF's mission is to enable IoT devices and services to communicate through a trusted open internet protocol (IP) framework which dynamically aligns with baselines for IoT security and privacy regulations, offering peace of mind and enriched experiences."

OCF collaborates with the IoT ecosystem to deploy and evolve the OCF ISO/IEC specifications, including the Secure IP Device Framework, its open-source reference implementation, and an industry-recognized certification program and label that:

- Enables secure end-to-end implementations that encompass device-to-device, device-to-cloud, and cloud-to-cloud
- Aids secure deployments with rapid development and simple integrations with IP networks and non-IP systems
- Fosters competition, facilitates productivity, and drives innovation
- Demonstrates conformance and trustworthiness to the industry and users
- Creates opportunities for secure and validated data to be pushed into Trusted Research Environments, facilitating the development of Information Management Frameworks to be used for greater operational insight

OCF sets itself apart from other standards, it is:

- An ISO/IEC standard
- Conforms to all known cybersecurity baselines
- Governed by leading companies in this space with transparent processes
- 500+ members representing the entire IoT ecosystem



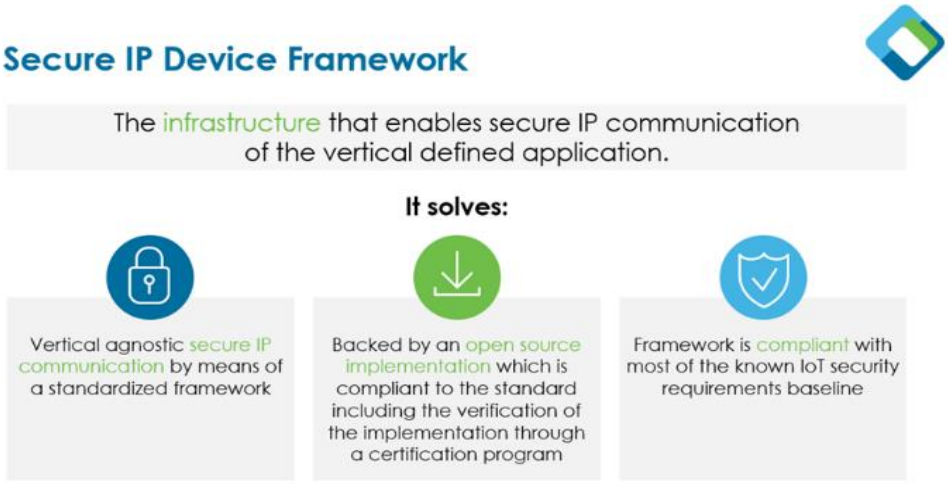
OCF Organizational Structure

"We want to position OCF as the default standard that governments will look to as part of their strategic vision for cyber physical infrastructure." Brian Bishop, President of OCF

The Secure IP Device Framework

The OCF Secure IP Device Framework enables device discovery, onboarding and application-layer security, for Device-to-Device and Device-to-Cloud IoT device connectivity. As an ISO/IEC adopted standard, this framework is internationally agreed upon by experts and is compliant with most of the known IoT security requirement baselines.

The Secure IP Device Framework utilizes the majority of the OCF standard used in the smart home, however, it strips away the data models, allowing it to be vertical-agnostic. The open-source implementation is easily accessible, and prevents vendor lock in.



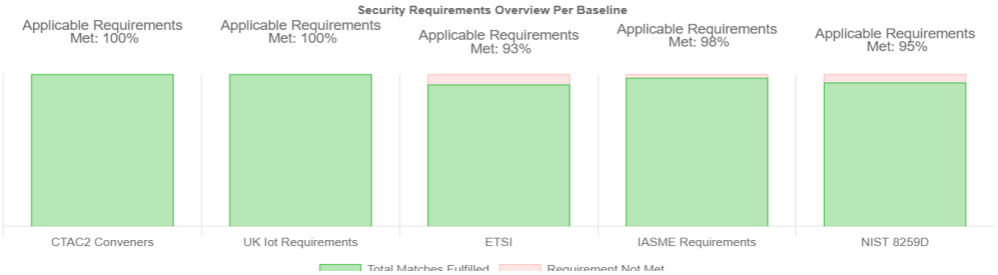
Benefits for governments & smart city infrastructures

'Security by Design'

The increasingly interconnected world and unsecure data streams increases potential exposure to cyber threats. To ensure the risk of cyberthreats originating from external sources is minimised, all OCF processes and systems are designed, implemented, built, monitored and run in such a way as to ensure security is fundamental. This allows for full integration with ISO/IEC specifications, including specifications such as ISO/IEC 62443 which specifies capabilities for automation control components.

- Met: The OCF Specification meets the clause or sub-clause of the baseline requirement with one or more OCF specification clauses
- Not Implemented: The baseline requirement is applicable to the specification, but is not currently met within the OCF specification
- Not Applicable: The baseline requirement is not applicable to the specification. Some examples of this are where the security baseline is out of scope for OCF, which is a device specification, or when the baseline requirement is implementation or user interface specific.

Note: Requirements that were deemed not applicable are not counted in the total percentages.



Interoperability – founded on a solid security framework

OCF offers validation from hardware to software, securing data as it flows from a device to a node. This path is often disjointed as a result of the patchwork of proprietary systems currently involved due a lack of trust between device manufacturers. OCF addresses the issues of cooperation and trust as the specification is publicly available and is designed to allow interoperability throughout.

Proof point: Working with FIWARE is an important step forward for the OCF in demonstrating its capabilities of offering specifications for smart city infrastructure and integrating outside models

'Compile your Compliance'

The current set of proprietary specifications in place is untenable. They have been created as a patchwork over time resulting in foundations which are weak and vulnerable to attack. IP based protocols and specifications ensure that specifications and the applications which use them work seamlessly and are highly secure.

The OCF has put in place traceable links between security legislation and the compliance of the OCF specifications to the legislation. As clauses within legislation are directly mapped to clauses within the OCF specification, and the OCF (conformance test tool) CTT verifies conformance to the specifications, implementations are assured to comply with legislation worldwide. Through this, users can Compile their Compliance.

Using a standard such as OCF helps ensure smart city architecture continues to operate seamlessly as it evolves in line with changing industrial communications standards. This is increasingly important as governance around access to data is changing rapidly, as evidenced by the UK Government's recent consultation on Data practices and review into delivering better, broader and safer use of NHS data.

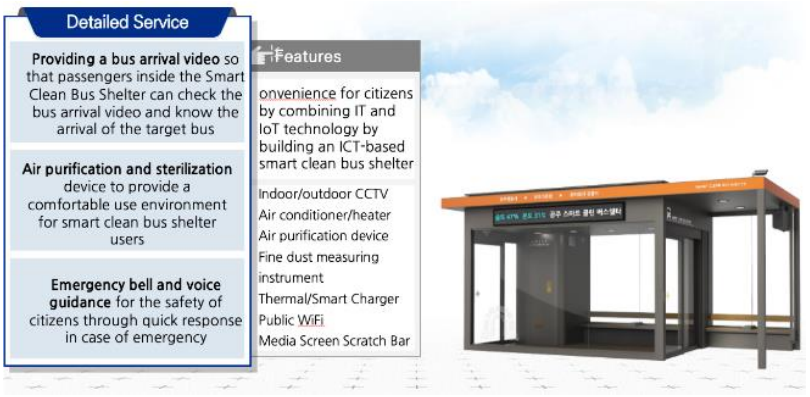
Enabling use-cases

The OCF Specification fits seamlessly into a digital twin model, allowing for a holistic approach to the management and optimization of urban infrastructure. This facilitates benefits such as:

- Multi-building energy management
- Traffic flow optimization
- Air quality control
- Occupancy Tracking

OCF in action

OCF Korea Forum member, Yungchang Co., Ltd., supported by ETRI, has developed smart bus stop and smart bus shelter solutions using the OCF standards. Following successful development, the solutions are set to be installed in cities across Korea through a series of government contracts.



Thanks to the traceable links between security legislation and the compliance of the OCF specifications to the legislation, the implementation is assured to comply with legislation not only in Korea, but worldwide.

This model demonstrates the benefits the OCF specification brings to the development of smart cities, and shows its potential for worldwide scalability.

Contact us to discuss how OCF can support your smart infrastructure development and research, with a framework built on trust, interoperability and secure communication.