

## **IPSO – IP for Smart Objects Alliance**

### ***Smart Objects – It's the future and it starts today***

Smart Objects refer to the wide variety of embedded devices capable of sensing or control and enabled with computing and communication capabilities. Through all walks of life, indoor or outdoor, in homes, offices, factories, streets or open fields and large-scale critical infrastructure, the wide-spread deployment of sensing, intelligent and communicating devices will have a tremendous impact on anything from public safety to reliable tracking of assets to improving health care to managing energy and monitoring and preserving the environment. The stakes around Smart Objects are all too important to all of us as citizens, industry players, service providers, educators or policy makers.

### ***IPSO Mission – Open Internet standards, and no excuses***

IPSO is an open industry alliance focused on promoting the use of open and interoperable IP networking standards for the new class of Smart Objects expected to pervade our lives. IPSO was founded to educate and foster interoperability around networking standards defined by the Internet Engineering Task Force (IETF). Many excuses have been used in the past for proprietary or ad-hoc standard approaches, usually on grounds of IP being only suited for “large footprint” devices such as computers. The IP architecture that has been highly successful as the convergence layer for most critical applications, including computing but also voice devices and services, mobility devices and services, video devices and services, and mission-critical control systems. Recent IETF standards have evolved IP protocols making them suitable for embedded and small footprint devices such as limited-resource and often battery operated sensors and actuators. IPSO is helping disseminate awareness that we can now “have our cake and eat it too”: build an open and interoperable ecosystem of Smart Objects that fit well with the rest of our IP-based information infrastructure without compromising on the performance and optimization requirements of embedded devices such as low complexity and cost, limited processing and memory, and often limited bandwidth or power budgets.

### ***Why Internet Protocols – A larger pie so everyone benefits***

It is critical to understand the reasons behind the success of IP as the convergence layer that has enabled the largest scale network every built and has absorbed new devices and services time and time again, previously thought “not to belong in the IP network”, whether in private and highly secure corporate or home networks or in large-scale public and wide-area infrastructure networks. Smart Objects are no different and hugely benefit from being IP-enabled end-to-end.

A common expression of the utility of a network is the so-called Metcalf Law, stating that the utility of a network is a function of the square of the number of devices that can interact over it. The architecture that maximizes the ease with which such interactions can take place across the broadest set of devices will maximize overall utility of networking. This is clearly the IP architecture.

### *Layered Architecture – Application Diversity, Media Diversity, Device Diversity*

The IP architecture provides a unique and scalable addressing, networking and routing paradigm that allows diverse applications to coexist (messaging, control, bulk transfers, real-time), on a highly diverse set of devices (computers, phones, mobile devices, sensors and controllers), each connected through diverse wired or wireless communication media types (Ethernet, Wi-Fi, DSL, Cellular, Cable, Low-Power Personal Area Networks). The key scale and investment protection aspect of the IP layered architecture is that it accommodates future inclusion of new media types, new device types, and new application types that apply to select devices, without inflicting “all or nothing” synchronized upgrades. This is in stark contrast with the “silo” architectures in which rigid inter-dependencies and assumptions are made from the top to the bottom of the stack and requiring that all participating devices be uniform and connected to the same network media, thus limiting things to a rigid set of capabilities and single media types, with an obvious lack of investment protection and future-proof evolution potential.

### *Link-Layer Independence – Largest Scope, Future Proof, Investment Protection*

The IP architecture is unique in enabling “mix and match” solutions to be built with devices deployed on heterogeneous media, some wired and some wireless, some low bandwidth and low power and some high bandwidth and high power, with benefits of flexibility and accommodation of future and improved media types. Recognizing and fostering adaptability towards “that which we know and that which we do not know” is key to evolving today’s investments rather than accepting stranded assets due to rigid and narrow assumptions around today’s state-of-the-art technology, which inevitably and rapidly becomes yesterday’s legacy and sub-par technology. What would be the utility of email or file sharing if Wi-Fi computers could only interact with other Wi-Fi computers in one way and needed different ways to interact with Ethernet attached computers? Similarly, what is the expected utility of Smart Objects if they’re segregated into islands of like-attached devices instead of securely but easily interacting with other Smart Object devices even those that are on different network media?

### *Innovation at the Edge – Fastest Innovation with Minimal Complex Dependencies*

By relying on end-to-end application and transport mechanisms and focusing the inter-networking functions between diverse sub-networks to a routing function, IP makes the network “non-intrusive” and transparent, with respect to innovative end-to-end applications that are developed on the edge devices served by the network.

**This is in contrast with complex protocol translation gateways needed when non-IP sub-networks with non-IP Smart Object devices need to interact with IP connected devices such as computers, servers, handheld and mobile devices. The innovation pace and price/performance improvements in IP-based Information Technology over the past few decades are a testimony to the resilience of IP networking in enabling those applications and devices that we know today, but also those that we cannot yet anticipate but need to have enabled for the future, when it comes to the network. If tomorrow's Smart Objects will beneficially and securely "twitter" or "file share" or "instant message" to each other, then let that be possible without requiring synchronized upgrades in intervening translation gateways!**

### ***Proven Scale Up and Down – Broadest Scale of Applications and Highest Utility***

**The IP architecture is capable of building small and cost-effective networks as is the case with existing home networks as well as enterprise-scale, country-scale or world-scale networks as is the case with corporate Intranets, government, defense and education networks and global-reach Internet backbones. Smart Objects are just as diverse in scope and scale: from home monitoring or patient monitoring contexts at small scale and complexity to campus facility monitoring contexts to utility-wide smart grid contexts to global asset tracking or environmental monitoring contexts.**

### ***Proven Security Models – IP and the Internet, Security through Obscurity Dead***

**IP networks and IP-enabled Smart Objects can be within private and highly secure networks or in Internet-connected and selectively secured and controlled networks. Some of the highest-impact and mission-critical networks are IP-based, whether in defense and classified communication or in banking transactions and stock trading or in factory automation and process control. The fact is, IP has the best understood security model and the most robust set of security mechanisms. Additionally, and thanks to its diverse link-inclusive and end-to-end application-inclusive capabilities, the IP architecture allows multiple and additive security mechanisms to be enabled on Smart Objects. As an example, a low-power wireless meshed Smart Object can have a strongly encrypted link layer security mechanism local to the mesh network, augmented with an end-to-end network-layer security mechanism such as "IPsec" (secure IP) or an application-specific end-to-end security mechanism such as SSL towards a remote Smart Object that may or may not be located on the same low-power mesh network. Importantly, the absence of a protocol-translation device in end-to-end IP Smart Objects removes a critical point of security vulnerability which more complex gateways introduce. In all cases, however, there is unanimous belief within cyber and information security ranks that "security through obscurity" and lack of protocol understanding is an utterly false and dangerous premise that cannot and must not underlie any mission-critical process or communication paradigm. IP-based Smart Objects have the opportunity to be the most secure Smart Objects, given the vast body of mature and proven security and defense techniques associated with end-to-end IP networking.**

### *Mature Deployment Tools – Manageability, Diagnostics, Skill Availability, TCO*

**Last but not least, the total cost of ownership associated with IP-based networks and Smart Objects is likely lower than that associated with ad-hoc and less pervasive network protocols. From the availability of trained, IP-savvy personnel, to the very broad set of products and tools for dynamic addressing, naming, tracing, querying, debugging, diagnostics and management, IP-based Smart Objects are likely to cause the least amount of “reinventing the wheel” and to leverage the most widely utilized and well amortized set of tools, in addition to saving training requirements on new and less pervasive networking paradigms.**

### *Join Us*

**Since its foundation in September 2008, the IPSO Alliance has rapidly grown to include leading participants across many industries and activity sectors. Some of the world’s largest or most innovative players have joined and continue to join IPSO at a rapid pace, representing diverse segments such as semiconductors, enterprise networking, software, hardware and services, electric utilities, automation systems, embedded sensing and control systems, utility metering systems, and academic and research institutions. Whether an end-user of technology, a service provider and integrator to end-users, or an equipment or component provider, joining us in IPSO and helping us promote IP-based Smart Objects makes you an active player in growing the pie of Smart Object related products and services. With your help, this will yield the best price / performance acceleration curves, of the kind that the Information Technology sector has yielded in unprecedented ways in the recent decades, for the benefit of end-users and industry players alike.**