Future Wireless Cities Workshop - Call for participation submission
Florence D. Hudson - Senior Vice President & Chief Innovation Officer, Internet2
fhudson@internet2.edu

Enabling a system of systems with end-to-end trust and security for Future Wireless Cities

Future wireless cities will include many types of smarter systems that can be leveraged in a “system of systems” and “network of networks” approach to maximize efficiency of the city and systems, while providing safety, privacy & security for the city and citizens.

The “system of systems” in smarter cities will communicate in an increasingly wireless fashion, supported by a wired backbone. Smart city “system of systems” will include smart grids, buildings, homes, transportation, tolling, connected/autonomous vehicles, M2M (machine to machine) and V2V (vehicle to vehicle) communications, public safety, emergency management, water management, integrated city logistics, and connected citizens. The “network of networks” supporting this “system of systems” has critical needs for advanced end-to-end trust and security to protect assets and citizens.

Internet2 as smart city testbed backbone
We will need greater citywide testbeds to test and connect systems within smarter cities, and to connect cities and communities, e.g., for distributed smart grid management. Internet2 and regional high-speed low latency secure networks can provide a backbone for the testbeds. NIST and Internet2 are discussing a smart grid testbed connecting “a grid of microgrids” including end-to-end trust and security working with universities, industry partners, regional networks, and government entities, as is the Internet2 legacy.

Smart city mesh network
Smart city systems will be deployed and connected through a smart city mesh network for mobile devices and people which we must define and develop. This network will include intelligence and applications to identify, assess, track, monitor and enable management of city assets and systems such as transportation systems through sensors and cameras to identify location and status of assets and people, leveraging location based services and relative position to other assets. The smart city mesh network will capture the location and disposition of cars, buses, trucks, trains, bicycles, emergency vehicles, and people through wireless sensor technologies and cameras. Vehicle-to-vehicle and machine-to-machine communications must be supported.

Extensible end-to-end trust and security open architecture
We need to develop an end-to-end trust and security open architecture for the “Internet of Things” to enable the smart city mesh network. The Open architecture is needed so all can deploy it, but it must include elements in the architecture that when executed will address Trust, Identity, Privacy, Protection, Safety and Security (TIPPSS). Adding new security features to the network, the endpoints, the systems and integrating processes are all in play. Elements of distributed trust between endpoints, ala blockchain, will be required for some systems. The network in future wireless cities will need to integrate many types of sensors and systems available today, with extensibility to include future sensors, systems and protocols that have not yet been envisioned or created.

About the Author
Florence Hudson created smart cities, grid, buildings, water management, and Internet of Things strategies at IBM before joining Internet2 as Senior Vice President and Chief Innovation Officer. She leads IOT and End-to-End Trust & Security Innovation Working Groups with university, industry, national lab, government agency, & network members.