SME Technology Development Program

Anchor Firm	ciena
Challenge Statement	**Security and Privacy of Energy Trading for Smart Grid**

Challenge Launch Date	November 6, 2019
Challenge Deadline	December 5, 2019
Challenge Statement	An efficient and robust Smart Grid is a necessity for secure energy trading. The technologies that enable Smart Grid are in early development stages. The goal for this project is to explore how Ciena can broaden the Smart Grid application space to Telecom Networks. For example, Smart Grid Communications will have to meet the QoS and QoE requirements of various applications. Global cloud computing has significant latency and cannot meet the need of real-time applications, edge computing is gradually being applied in Smart Grid. The project will evaluate several technologies (Blockchain, Artificial Intelligence / Machine Learning (AI/ML), Deep Learning algorithms to provide a solution for secure energy trading in a Smart Grid environment and to apply to a specific Use Case.
Project Partner	Ciena Canada
Timeline	2 years
Available funding	Up to $250,000 CDN
Applicant Type	Ontario based SME Scale company
Location	Flexible, Ciena team is based in both Ottawa, ON and Montreal, QC
Project Details	The continued increase of power consumption, diversity of power grid, electric vehicle services, and many device/user interactions is driving the requirement for optimized energy transition and energy efficiency. The key is to promote local energy production, and avoid the energy transport loses over long distances. Promoting local energy production means the integration of renewable energies within the existing network. However, this integration requires good management because wind and/or solar energy generates electricity intermittently, which is why digital management is essential in order to achieve a stable electrical system. This digital management is the Smart Grid that relies on automation and seamless and remote access. Ultimately, Smart Grid will have to coordinate an energy market of all types of energy from diverse sources, renewable or not renewable, from local production to a remote

	production. In addition, a Smart Grid infrastructure must enable an efficient, secure, and transparent pricing model.
	
	A secure peer-to-peer energy transaction between producer and consumer in the same micro-grid will be an efficient solution.
	
	Security, privacy and not refutable transactions are the key enablers for such a market.
	
	The intent of this project is to provide an optimization mechanism, solution and algorithms for **secure energy trading** for a Smart Grid EV (Electric Vehicle) Use Case, evaluated on the following parameters:
	
	• Security: the security mechanisms that must be in place are:
	  ○ Authentication – verification of an entity joining the micro grid technology is who they say they are.
	  ○ Authorization – verification that the entity who does join has the authority to do what they plan to do.
	  ○ User management
	  ○ Directory & Namespace management
	• Privacy : Identity for the participants, and their private and trading data, need to be secured and protected:
	  ○ Data protection
	  ○ Privacy policy
	• Not Refutable transaction: transactions in the system need to be:
	  ○ Validated
	  ○ Stored
	  ○ Benefit of the transaction completion need to be proofed
	
	In the course of this project a set of technologies (e.g. Blockchain, Artificial Intelligence / Machine Learning (AI/ML), etc..) needs to analysed in order to provide a solution for **secure energy trading** in a Smart Grid environment. A solution will have to be designed and developed. Various Machine Learning algorithms should be explored, including reinforcement learning, Long Short Term Memory (LSTM), Deep Q-networks for security and identity management.

Project Goals/ Outcomes	Expected project outcomes: • An architecture based on blockchain and AI/ML • A set of AI/ML algorithms for a) Security, b) Privacy and c) Non refutable mechanism for transactions • A software framework supporting the selected architecture • A working proof of concept for an EV (Electric Vehicle) Use Case Anticipated project timeline:

	• 6 months - Review and test initial software in our lab and start DEMO development; • 12 months – Development of the Edge Artificial Intelligence algorithms and Application Controllers • 18 Months - Development of the required Control loops and Edge Optimization Framework • 24 months – Final Review & Report, Transfer of Knowledge, and software
Applicant Capabilities	The applicant SME should have the following capabilities: • Comprehensive understanding, and hands-on experience with Artificial Intelligence and Machine Learning • Comprehensive understanding of blockchain technologies • Comprehensive understanding of Identity Management and Security Management • Deep Knowledge on SmartGrid architectures • Knowledge in the following areas: Software Architecture, Blockchain, Big Data Analytics, Data Analysis and Modeling, Artificial Intelligence coding • Technical background with the ability to understand a wide variety of technologies, standards, and product applications • Experience with software and complex systems test
Additional Information	Work in collaboration with Ciena Canada's CTO team

Launched in 2018, the ENCQOR 5G SME Technology Development Program partners Ontario based SMEs with ENCQOR 5G Anchor Firms on 5G technology development projects. Areas of research interest are defined by Challenge Statements submitted to OCE by the ENCQOR 5G Anchor Firms and posted to the OCE website on a rolling basis.

If you are interested in developing an expression of interest, please visit the program guidelines for information on next steps.

For any questions about new Challenge Statements or the ENCQOR 5G SME Technology Development Program please contact Jennifer Moles at Jennifer.Moles@oce-ontario.org.