

# Module-OT: Modular Security Apparatus for Managing Distributed Cryptography for Command and Control Messages on Operational Technology Networks




*Securing distributed energy resource systems with lightweight, low cost, and vendor-agnostic cryptographic modules*

Increased levels of renewable energy and other distributed energy resources (DERs) on the electric grid have introduced new cyberattack vectors and increased the attack surface across modern energy systems. Recognizing this challenge and the critical need for an energy infrastructure, this project develops a solution to better protect data and communications on the distribution grid that provides security to both information and operational technology systems. Module-OT improves system security through encryption, authentication, authorization, certificate management, and user access control. It utilizes the latest industry standard hardware acceleration that improves the overall communication performance in terms of end-to-end latency. It is a lightweight module with interfaces that allow the technology to be embedded into power system devices of all sizes, including photovoltaic inverters. This technology mitigates threats from man-in-the-middle attacks and other forms of unauthorized access across increasingly diverse, complex, and expansive DER infrastructures.

---

## KEY TAKEAWAYS

- Designs and develops software-based interfaces to embed cryptographic services using public key infrastructure within distributed energy resources
  - Delivers low-cost and vendor-agnostic solutions for resource interoperability, cybersecurity, and easy management of distributed energy resource systems
  - Creates technology to ensure low-latency cryptography for fast authentication
- 

## OUTCOME

This project delivers a cryptographically secure module that enables electric utilities, DER asset owners, and aggregators to seamlessly integrate or retrofit DER devices. Embedding cryptographic services on top of pre-existing equipment also allows for customization, such as selective encryption based on a pre-established threshold for sensitivity or low-latency application, as well as module replacement without retiring equipment.

## PARTICIPANTS

## ROLE



Designs, develops, and validates the module; provides overall technical direction based on team consensus



**Sandia  
National  
Laboratories**

Evaluates module performance in an emulated environment and performs penetration testing



**Public Service  
Company of New  
Mexico**

Supports validation of the module by providing access to a 500-KW PV plus storage facility for use as a test site



**SOLECTRIA**  
A YASKAWA COMPANY

Improves module design and characteristics for better integration with DER devices

## CONTACT INFORMATION

### Initial Leads:

**Carol Hawk**  
Program Manager

**Danish Saleem**  
Principal Investigator  
National Renewable Energy Laboratory  
720-404-5912  
[danish.saleem@nrel.gov](mailto:danish.saleem@nrel.gov)

### Current Contact as of February 2020:

**Akhlesh Kaushiva**  
Senior Technical Systems and Cybersecurity Advisor  
Department of Energy (DOE)  
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)  
202-287-6062  
[Akhlesh.Kaushiva@hq.doe.gov](mailto:Akhlesh.Kaushiva@hq.doe.gov)

**Period of Performance:** October 2017 – May 2021

**Total Award Value: \$2,575,000**  
DOE Share: \$2,575,000  
Cost Share: \$0

### CYBERSECURITY FOR ENERGY DELIVERY SYSTEMS (CEDS)

CEDS projects are funded through DOE CESER, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyberattacks.

Website: <https://www.energy.gov/ceser>

Date Written: June 2021