With increasing deployments of smart grid systems, a large quantity of energy usage and grid status data have been collected by smart grid devices like smart meters. To secure these critical and sensitive data, it is crucial to prevent unauthorized readings from these devices. Many authentication protocols have been proposed to control access to smart grid devices that are a part of the smart grid data communication network; however, authentication protocols to control readings from the isolated smart grid devices are mostly ignored In this paper, we propose a secure and efficient framework to enable secure data readings from the isolated smart grid devices based on a two-phase authentication protocol, The framework not only makes use of the smart reader as a bridge to connect the isolated smart grid device and the smart grid cloud, but also considers the physical constraints of all the devices in the systems. Security analysis shows that our framework is efficient and secure under most typical attacks, meanwhile it satisfies the hardware constraints of smart grid devices. Comprehensive performance evaluation also validates the efficiency of the proposed framework.