WHITE PAPER

Scalable, Secure and Integrated: Rethinking Provisioning for Utility Networks

By Daniel Allnutt and Mat Eshpeter

Strategic provisioning is key to scaling private LTE networks in utilities. Beyond zero-touch provisioning models for automation, success at utility scale depends on integrated systems, robust security and alignment with IT/OT operations to minimize manual effort, risk and complexity.

Utilities across the United States are increasingly adopting private LTE (PLTE) networks to improve the performance, security and reliability of their operational communications. With this shift comes an often overlooked but critically important technical challenge: provisioning.

To successfully scale a PLTE deployment, utilities must consider a comprehensive provisioning strategy that integrates multiple systems, supports automation and minimizes manual intervention. In creating its provisioning system strategy, a utility might have to consider whether it has dedicated technical resources available to handle the provisioning system's deployment and ongoing maintenance. Zero-touch provisioning (ZTP) models offer a transformative opportunity for utilities seeking to scale PLTE networks efficiently and securely, but it requires careful design, given each device's need for certain preliminary information before the device can pull its configuration over the air.

Role of Provisioning in PLTE

Provisioning in telecom refers to the process of securely onboarding and configuring devices to let them access and utilize network services. In a PLTE environment, this effort includes not only onboarding the devices but also configuring the underlying infrastructure that supports authentication, encryption, and device and associated IED controller addressing. Unlike carrier-grade provisioning systems that support millions of consumer devices and tie into complex billing platforms, utilities operate in a more static and focused context. Their provisioning needs should be tailored to their operational environment, where reliability, security and process alignment are more critical than high-volume scalability.

The PLTE team at Burns & McDonnell has performed lab testing for PLTE provisioning, centered on understanding what it takes to enable device onboarding with minimal manual input. This includes evaluating the provisioning of subscriber information into the home subscriber server (HSS), managing device configurations through vendor-specific element management systems (EMS), and establishing secure tunnels for data transport using protocols such as internet protocol security (IPSec).

Promise and Limits of ZTP

ZTP aims to eliminate manual configuration steps during device deployment. In principle, a device could be powered on, connect to the network and automatically receive its configuration. This concept was explored in a series of lab tests, working with multiple vendors to identify practical implementations. Common approaches included:

- Factory preconfiguration of user equipment.
- QR code scanning for bootstrapping.
- USB drive-based initial configurations.
- Cloud-based provisioning platforms.

Each method presented trade-offs. For example, when running on PLTE networks, many devices required a manually preloaded access point name (APN) to receive an IP address and initiate communication with a provisioning server. Without this minimal bootstrap configuration, the ZTP process could not proceed. Some vendors implemented cloud-based registration, but this approach could introduce security concerns and assumptions about internet connectivity that might not align with utility environments.

To realize the full benefits of ZTP, utilities must look beyond isolated configuration automation and develop a comprehensive, integrated provisioning framework. True automation in PLTE provisioning requires integration across several domains. The goal is not just to push device configurations automatically, but to weave provisioning into a larger system of operational technology management, network life cycle workflows and enterprise IT governance.

A complete device onboarding workflow (Figure 1) may involve:

- Initiating a work order for deployment.
- Associating a SIM card with a device and recording metadata (IMSI, IMEI).
- Uploading configuration data to the device EMS.
- Assigning IP addresses through integrated IP address management (IPAM) systems.
- Leveraging public key infrastructure (PKI) to implement a device certificate strategy to support activating IPSec tunnels and other security needs.

Managing Risk and Maintaining Security

Provisioning touches on multiple points of trust and security. Observations from lab testing highlighted cases where provisioning flows lacked mutual authentication or encryption at early stages. Such vulnerabilities raise questions:

- Do utilities trust vendors or third parties to preload configurations?
- Is mutual certificate-based authentication in place?
- Are cloud-based provisioning platforms acceptable for OT-critical devices?

Risk tolerance will vary by utility, but every provisioning solution should be vetted with security principles in mind. It is essential to assess not only the technology but also the operational processes and related systems supporting the provisioning process.

An effective provisioning system for utilities should integrate with existing IT/OT processes, minimize additional tooling and support the life cycle management of devices. Rather than adopting public telecom provisioning platforms built around public network requirements, utilities can leverage existing asset databases and related processes to support their specific PLTE device management requirements. Extending the capabilities of a utility's existing asset management system to support PLTE provisioning might not be onerous, given provisioning interfaces are RESTful APIs

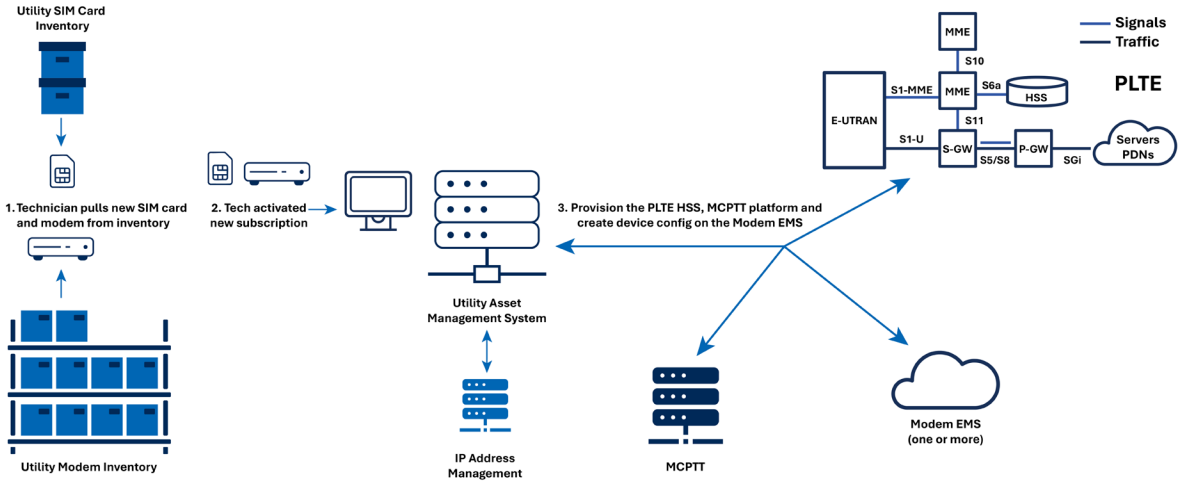

*Figure 1: **Sample provisioning flow.***

(representational state transfer application program interfaces), which are simple and well-known programming interfaces.

Ultimately, the provisioning strategy must reflect the operational priorities of the utility: high reliability, strong security and scalability. With automation and thoughtful integration, provisioning becomes a strategic enabler rather than a deployment bottleneck.

Designing a Utility-Grade Provisioning Strategy

Provisioning for PLTE networks is a complex and multifaceted challenge that extends well beyond zero-touch device provisioning. While a ZTP philosophy provides a foundation for automation, an end-to-end provisioning strategy requires deeper system integration, robust security frameworks and alignment with utility operations.

By addressing these layers systematically, utilities can streamline network rollouts, improve maintainability and safeguard critical infrastructure. Lab testing underscores that the path to scalable PLTE provisioning is achievable but requires rigorous planning and a holistic perspective. By making intentional decisions around architecture, automation and vendor trust, a thoughtful provisioning strategy provides a clear pathway to operational excellence.

About Burns & McDonnell

Burns & McDonnell is a family of companies bringing together an unmatched team of engineers, construction and craft professionals, architects, and more to design and build our critical infrastructure. With an integrated construction and design mindset, we offer full-service capabilities. Founded in 1898 and working from dozens of offices globally, Burns & McDonnell is 100% employee-owned. For more information, visit **burnsmcd.com**.

890056568-0925