



# JI Technology – Access Control

Device & SIM Check/Authentication

## JI Technology

Founded in 2008 to provide solutions and business development for MNO, MVNO, System Integrators & Service Providers, these solutions include charging, messaging, gateway applications and service control solutions. Our current & past engagements include Prepaid, Loyalty, Multi Payment Channel service, IOT, SMS gateways, EPC for sXGP/private networks/EDGE, Fintech consulting & others.



### INTERNET OF THINGS

We are mapping out IOT value for those who are ready to act



### PRIVATE EPC

Complete solutions for the enterprise, integrators, for service providers



### sXGP

Reducing the cost of telecommunications services and improving the stability of wireless communication services



### BESPOKE SOLUTIONS

Competitive & agile. Presales through delivery

## Access Control for sXGP/uLTE enterprises

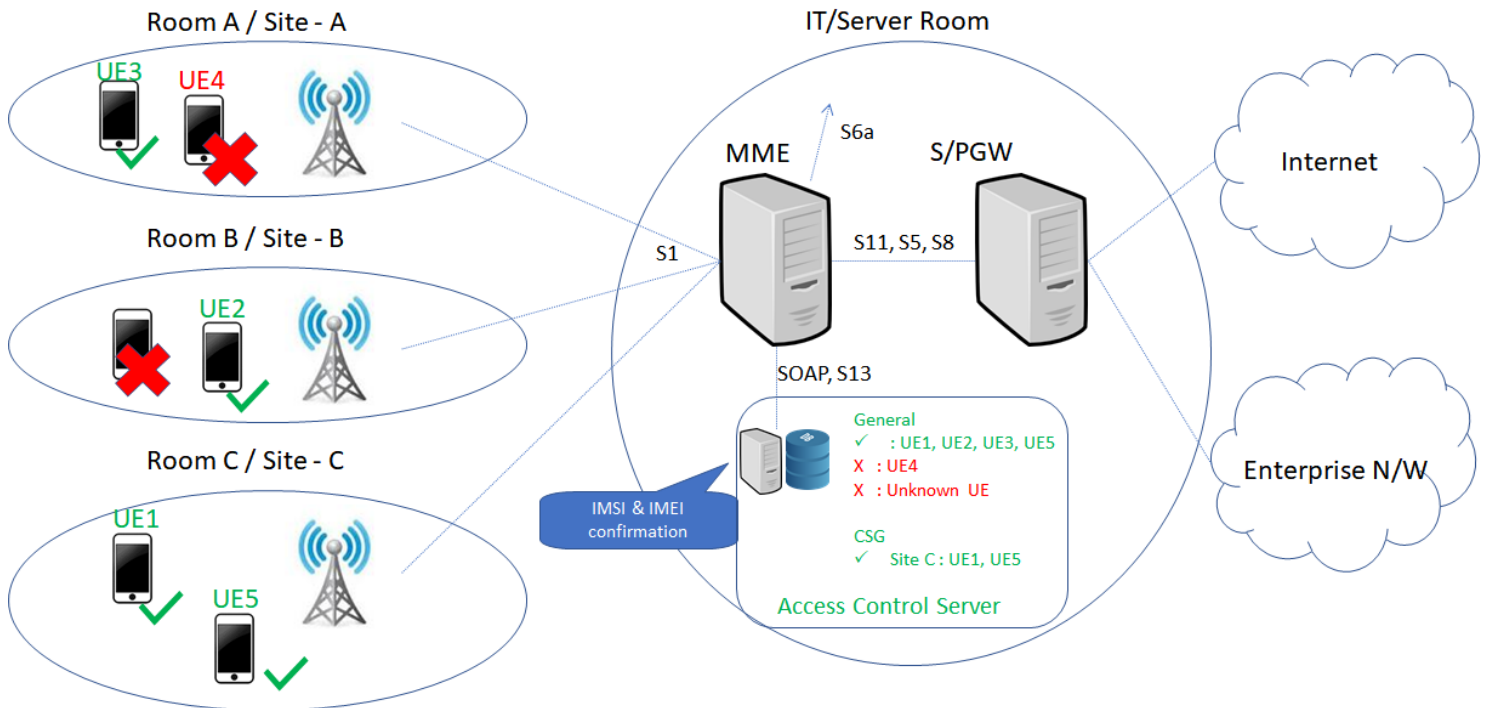
Access control ensures use of authorized devices on the enterprise network by checking both the IMSI of the SIM card, the IMEI of the device & the ENodeB that the device is accessing. This helps to restrict enterprise network access to only approved devices and users. Un-restricted devices and users are security risks that can bring malware, viruses into a network and also unauthorized access to the enterprise.

### Why UE access restriction?

Private LTE allows devices to directly access an Enterprise network and Enterprises must be cognizant about the potential threats on the horizon. Typically, enterprises are unable to enforce a BYOD policy due to the devices being managed by public operators, but this dynamic changes with private LTE.

- With the introduction of private LTE networks, enterprises & institutions of all sizes can now block BYOD by controlling UE & SIM that can be used to access to their private network
- Additionally, the Access Control server enables a type of subscriber group management per eNB. For a closed eNB, only allowed members (IMSI) may be attached via the eNB.





## Access Control for “private LTE/uLTE/sXGP/Multifire”

The JI Access Control Server brings the 1<sup>st</sup> level of security check to the private enterprise network by ensuring only the authorized uLTE Device & SIM can attach to the network at the specified location. This happens even before the IMSI authentication with the HSS / devices attaches to the network. The Access control server has been designed to satisfy the needs of organisations and facilities that need to tightly control access to mobile networks and services in a defined area.

- Verified with the sXGP environment (EPC, eNB, UE, SIM)
- Supports network planning and monitoring
- Multiple MME per Access Control Server
- Ready for use in both 4G & 5G environments
- PCS-DSS compliant for information storage, access
- Checks IMEI & IMSI & eNodeB before HSS authentication
- Enables multiple sXGP/uLTE networks to operate in similar area by redirecting IMSI with relevant EMM code
- Reject standard PLMN SIM/IMSI attach attempts with suitable/configurable error codes
- Welcome/Onboarding SMS: detects 1<sup>st</sup> time access for a user and sends pre-defined SMS
- Broadcast SMS to all UE actively attached to specified eNodeB
- Online update to add/update/remove entries
- Different Cause Codes per IMSI/IMEI
- Per MNC/MCC cause code return
- Create Closed, Hybrid, Open enodeb/Access Points for subscriber groups & area controlled access
  - Assign allowed IMSI to each Access Point ID
  - Broadcast SMS to all UE in a subscriber group
- On-Premise/Cloud options
- Analytics via real-time logging/GUI to see illegal & Valid device access requests
- Visit us at <http://www.jitechnology.com>