



CORNING

# Enterprise RAN

## Security Built from the Ground Up

Security cannot be an afterthought. It is critical that manufacturers are able to anticipate and address the security concerns of all customers, including government regulators, law enforcement, mobile operators, and enterprise IT security teams. Corning has accomplished this with the design of its SpiderCloud® Enterprise RAN (E-RAN) platform.

When small cellular base stations (called small cells) are deployed in an environment where untrusted people may have physical access to them, they must be designed as closed, secure systems that are resistant to physical or local/remote digital attacks.

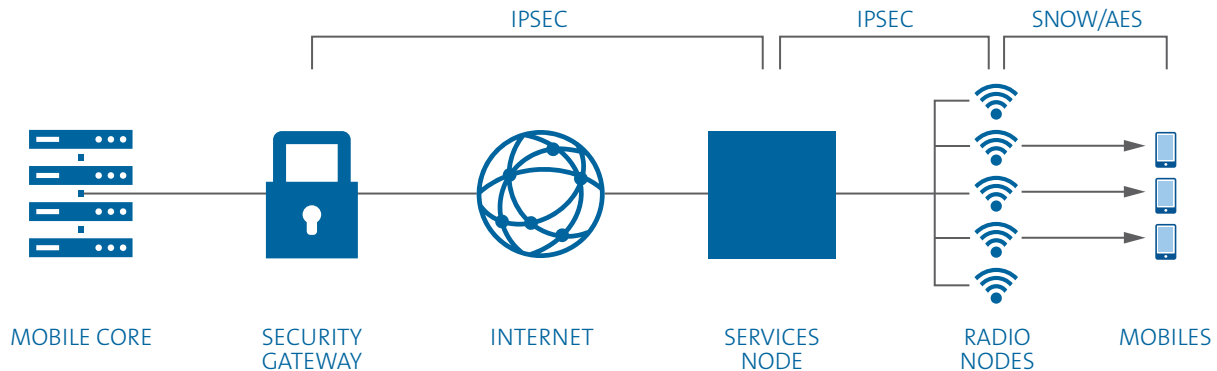
Security is an integrated part of the design process, as adding security on later can be impossible when a software security technique has a dependency on hardware subsystems that must be present.

### Mobile operators are regulated by government and must comply in multiple areas:

- **Subscriber privacy** – No subscriber information or data flows will be visible on the network.
- **System security** – The integrity of the cellular network will be protected at all times.
- **Law enforcement** – Commission on Accreditation for Law Enforcement Agencies, Inc. (CALEA®) laws provide for lawful intercept capability, and RAN systems must not indicate lawful intercept activity.
- **Public safety** – E-911 services will provide the PSAP and first responders with indoor location of callers within 50 meters of call origination location.

## Enterprise RAN (E-RAN) Platform Security

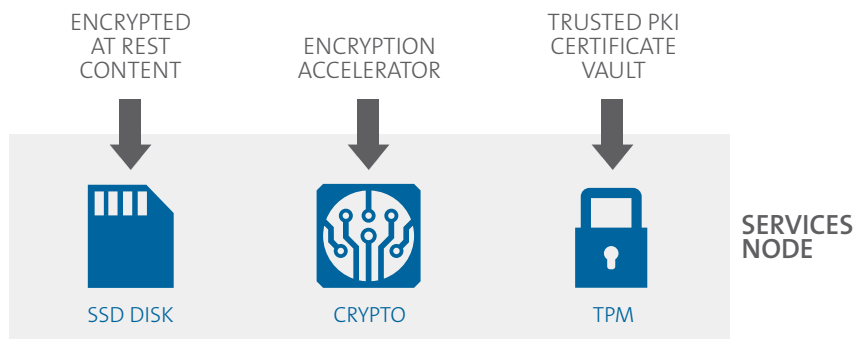
Each E-RAN system consists of up to 100 radio nodes (RNs) connected to a services node (SN). RNs securely connect over an enterprise Ethernet local area network (LAN) and/or a virtual LAN (VLAN) to the SN. The SN originates a single secure connection to a security gateway at the edge of the mobile operator's core network over high-speed IP transport.



Think of the SN as a secure system that implements 3GPP standard encryption over the air between the mobile devices and attached RNs, IP/IPSec on the Ethernet to the attached RNs, and IP/IPSec on the transport network between the SN and the security gateway(s) at the perimeter of the mobile operator's core network. The 3GPP-defined Kasumi and Snow air link protocols are used between the mobile devices and E-RAN.

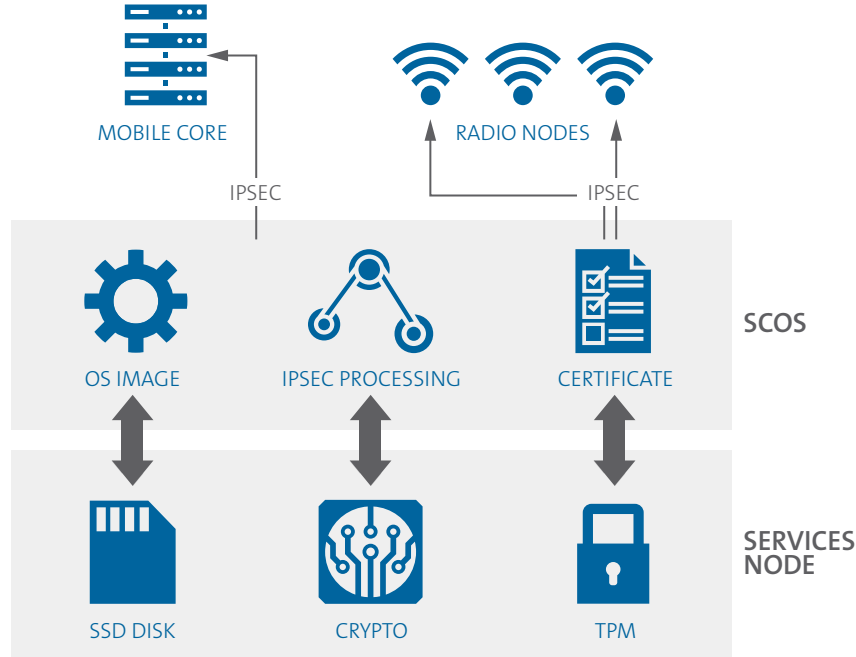
Working from the ground up, the system hardware incorporates both tamper resistance and secure repositories that anchor secure software elements:

- All the normal disabling/fuse blowing (manufacturing/diagnostic interfaces – JTAG) is done to many of the critical semiconductors. This prevents abuse of development and manufacturing test equipment to exploit them.
- TPM vault on the SN and all RNs to store PKI certificates. TPM vaults are used extensively to protect PKI private keys from export from the hardware. This is critical to maintain trust that attackers cannot quietly develop eavesdropping capabilities by compromising IPsec security.
- SN uses a network processor with hardware acceleration for IPsec, not a general-purpose processor.
- Encryption of all data at rest in SN storage prevents any attacker from recovering data from the SSD drive.
- The local console interface on the SN is scope-limited as an installation bootstrap interface that is remotely disabled after commissioning an E-RAN system.



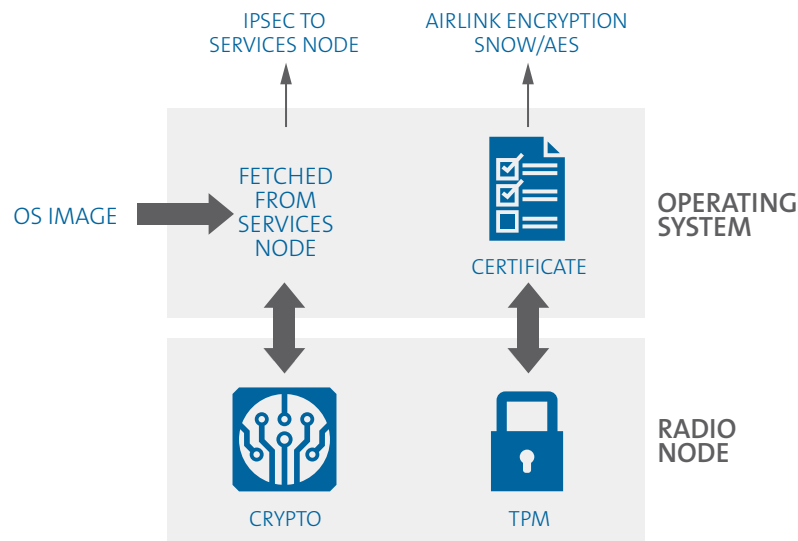
The SpiderCloud® OS (SCOS) in the SN leverages the following hardware features to protect itself and the privacy and integrity of the traffic flows between the mobile devices and the mobile core.

- E-RAN hardware will only load factory-signed code images that must successfully validate against the PKI key resident in the RN or SN TPM vault.
- All PKI certificate public/private keys are secured from export via storage in TPM.
- Support is available to use default factory-provisioned certificates or operator certificates.
- OSCP or CRL methods are available to determine revocation status of the certificates in the hardware.



The RN is a very sophisticated part of the overall system and has a broad range of protections built into it.

- An RN has no resident operating system and fetches it, at power up, from the SN. Stolen RNs cannot do anything because they do not have an operating system.
- Each RN for a site has a Layer 2 MAC address that is part of the SN configuration.
- The SN and RN mutually authenticate each other as part of building their IPsec connection. This is a protective measure that prevents a man-in-the-middle attack. The RN's operating system is signed and must validate against the hardware during boot process or it will not load.
- There is no console interface on an RN. It only has an Ethernet port that expects to be connected to a PoE+ port on an enterprise LAN/VLAN.



In the E-RAN, IPsec and 3GPP features for path protection and integrity are key to ensure service availability and subscriber data privacy.

- IPsec is utilized between SN and its RNs, and between SN and the mobile operator security gateway (SeGW). Even when private transport (MPLS, metro Ethernet) is being utilized by an operator, IPsec is used to preserve privacy of subscriber payload.
  - An SN can connect to multiple SeGWs for fault tolerance. The SeGWs can also be geo-redundant to protect from cable cuts and power problems that can affect data centers.
  - Extensive QoS policy controls over all backhaul access inside the IPsec path and DSCP marking for MPLS CoS handling enable the SN to protect critical traffic when the backhaul experiences congestion.

Security auditing is the final step in ensuring that the system is continuously delivering both confidentiality and integrity of subscriber traffic traversing the system.

- E-RAN is audited and penetration tested routinely by a third-party specialist security vendor as part of QA processes. Any issues found are remediated.
- System is routinely audited/explored by our mobile operator's technology security team as part of due diligence.
- System hardware and RAN protocol use standards to connect to both the mobile device over air link and the mobile core via security gateway. This means Corning has done a significant amount of interoperability testing with mobile devices of many varieties, SeGW, and evolved packet core (EPC) vendors.

Bolt-on security implies an afterthought. Security should NEVER be an afterthought. Corning's scalable small cell system makes use of a built-in security approach in its system design, from the ground up, to ensure that it meets the demands of both mobile operators and enterprises.

Learn more at  
[www.corning.com/smallcell](http://www.corning.com/smallcell)

The Corning logo consists of the word "CORNING" in a white, serif, all-caps font, centered within a solid blue square background.

CORNING

Corning Optical Communications LLC • PO Box 489 • Hickory, NC 28603-0489 USA  
800-743-2675 • FAX: 828-325-5060 • International: +1-828-901-5000 • [www.corning.com/opcomm](http://www.corning.com/opcomm)

Corning Optical Communications reserves the right to improve, enhance, and modify the features and specifications of Corning Optical Communications products without prior notification. A complete listing of the trademarks of Corning Optical Communications is available at [www.corning.com/opcomm/trademarks](http://www.corning.com/opcomm/trademarks). All other trademarks are the properties of their respective owners. Corning Optical Communications is ISO 9001 certified. © 2019 Corning Optical Communications. All rights reserved. CMA-687-AEN / January 2019