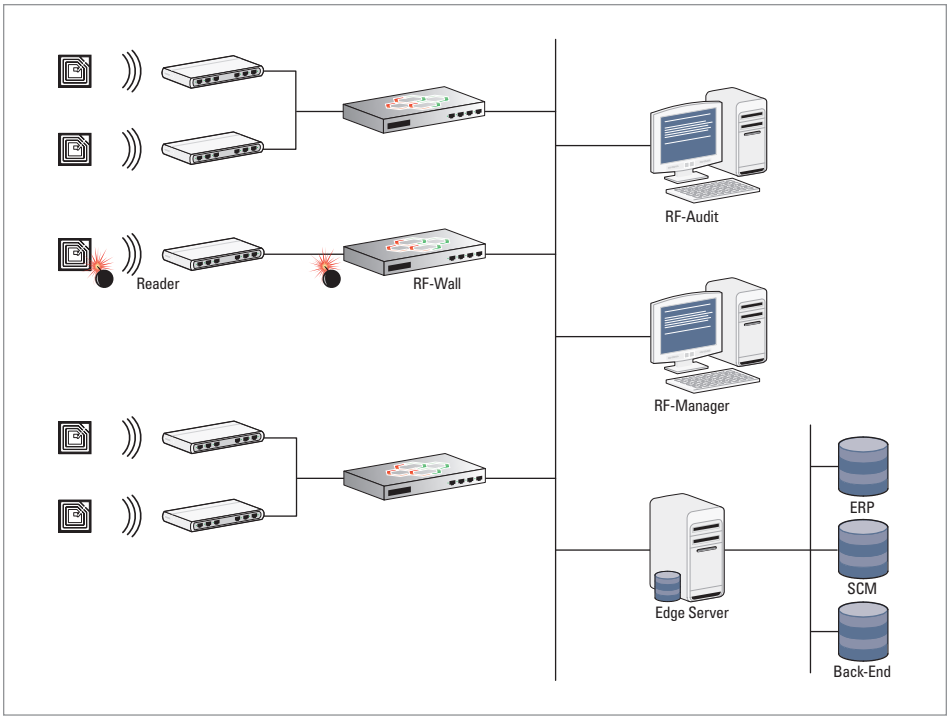
RFID technology promises great advantages over traditional bar code applications. Instant visibility without line of sight allows for powerful supply chain and inventory management applications. Cash cards and electronic tickets based on RFID technology have become common place due to their convenience and product authentication applications for high-value items are designed to help deter fraud and theft.

Yet, RFID technology opens new venues for attack. The situation of the RFID industry today compares to the early days of the Internet where the benefits of a new technology were clearly visible but there was little awareness that corporate networks need to be guarded by firewalls and personal computers should be protected by virus scanners – these security concepts had yet to be invented.

Without any safeguard in place the benefits of an RFID application may be outweighed by fraudsters exploiting new security holes. You may already be victim to fraud without even knowing it, because you lack the auditing capabilities to identify incidents after they happen let alone quantify them. Cash cards or tickets may be duplicated or recharged illegally. Counterfeit parts may find their way into the supply chain and use cloned RFID tags to pose as genuine original parts. Key cards may be scanned and copied using off-the shelf hand-held devices by simply bumping into a person carrying the original key in his pocket. Business critical backend systems may be infiltrated, disrupted or otherwise compromised by Malware




spreading via RFID tags. As a result of these types of attacks your business may get hurt in different ways, for example:

» Revenue loss due to cheaper counterfeit products (grey market)
» Brand damage due to counterfeits of inferior quality
» Disruption of business operations due to failure of key backend systems
» Loss of trade secrets due to infiltration of backend systems

The NeoCatena Security System provides all you need to mitigate and mange security risks inherent to RFID technology. We see RFID as a network and draw on lessons learned securing the Internet. In fact, you can think of RF-Wall as a firewall for RFID. RF-Wall is a flexible security appliance that can be configured to:

» Check if tag data has been tampered with or if tag data has been cloned by copying data from a genuine original tag to an unauthorized second tag
» Make sure all tag data is encrypted when writing to the tag (and decrypted when reading it back)
» Scan tag data for known attacks (RFID Viruses, SQL Injections and other forms of Malware) designed with the criminal intent to infiltrate, disrupt or otherwise compromise your edge servers and backend systems
» Perform statistical analysis and plausibility checks to identify unusual activity
» Send alerts for immediate response or log incidents for later auditing and compliance with industry regulations and governing law

RF-Wall integrates seamlessly with existing legacy applications. Our flexible connector architecture lets you plug RF-Wall into existing RFID applications without the need for any hardware or software adjustments. This means you can add proven state-of-the-art security to new or existing applications in no time without having to worry about implementing or maintaining anything yourself – leaving you more time to focus on your core business.

Whether your goal is to add a bullet proof layer of security to an existing application or whether you are starting from scratch, NeoCatena is your partner for every aspect of RFID security. We help you plan and design applications with security in mind from day one and are available to guide you through implementation to production and beyond.

## KEY FEATURE MODULES

| | |
|---|---|
| **Encryption / Decryption** | » AES<br>» DES, 3DES<br>» Blowfish<br>» SEED |
| **Digital Signature / Tamper Detection** | » Online / Offline Signature with Timestamp<br>» HMAC-SHA-1/SHA-256<br>» HMAC-MD5<br>» HMAC-RIPEMD-160 |
| **Data Validation** | » Standard Encoding Validations<br>» User Defined |
| **Error Correction** | » Checksum based ECC |
| **Threat Detection / Filtering** | » Generic SQL Injection<br>» Known Exploit Signatures<br>» Blacklist<br>» Whitelist<br>» Tag ID Pattern Filter<br>» Custom Attack Signature |
| **Custom** | » RegEx<br>» Perl Script |

## MANAGEMENT

| | |
|---|---|
| **Management** | » RF-Manager (desktop management client software)<br>» HTTP Web Management Interface<br>» REST Web Services<br>» SSHv2 CLI<br>» SNMP |
| **Logging / Auditing** | » RF-Audit (desktop audit client software)<br>» Reporting Engine<br>» SysLog<br>» SQL Auditing Database |

## SUPPORTED PROTOCOLS AND STANDARDS

| | |
|---|---|
| **Tag Types** | » ISO 14443 A/B/C<br>» ISO 15693<br>» MIFARE (UltraLight, Classic, DESFire)<br>» EPC C1G2<br>» ISO-18000 6c<br>» DoD Layout |
| **Reader Protocols** | » Phillips MultiISO, DualISO and PC/SC<br>» LLRP<br>» Alien Reader Protocol<br>» RF-Wall XML REST<br>» RF-Dump XML<br>» Custom |

## HARDWARE SUMMARY

| | |
|---|---|
| **Display** | » 16x2 character LCD display |
| **Connectivity** | » 6 Gigabit LANs ports<br>» 1 port USB / RS232 (loop through) |
| **Form Factor / Dimensions** | » 1U rack mount chassis<br>» 44mm (H) x 430mm (W) x 411mm (D) |
| **Certifications** | » CE/FCC |