LG GATE

Guarded Access To Enterprise

LG
Life's Good

LG GATE

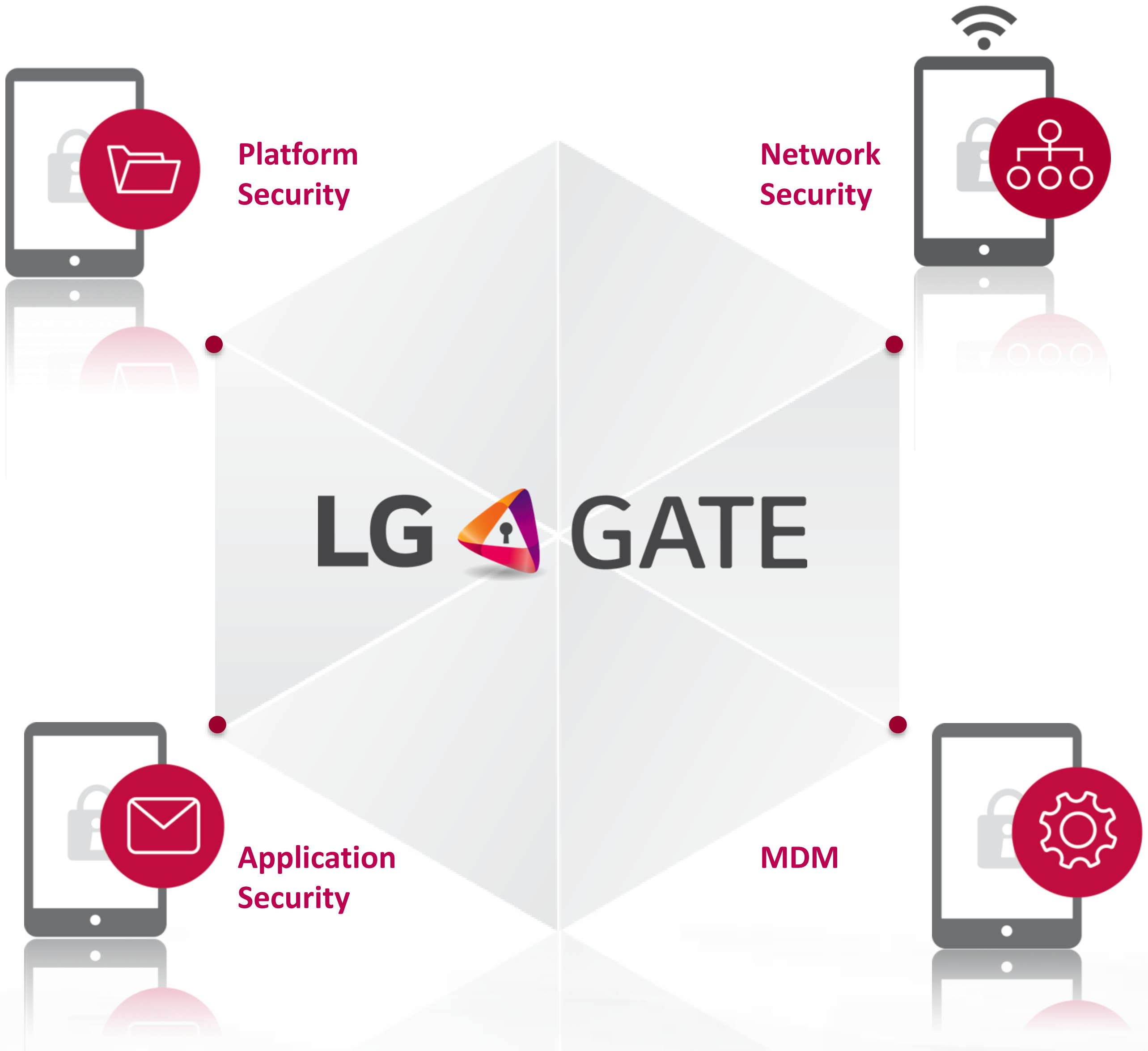
(Guarded Access To Enterprise)

In the era where mobile devices are increasingly used for business needs, LG GATE provides peace of mind to both corporate IT managers and employees. With powerful capabilities and government-grade security, LG GATE creates a secure and efficient mobile work environment for all users.

LG GATE

LG Enterprise Solutions

LG GATE is comprised of four enhanced technologies of core enterprise solutions which will enable the security and manageability of enterprise data.



LG GATE CONTENTS

Platform Security

- Enhanced Secure Boot
- SE Linux
- Enhanced Data Encryption
- H/W Accelerated Encryption
- Enhanced Key Management
- TZ-based Certificate Management

Network Security

- LG VPN
- Enhanced Certificate Validation

Application Security

- Enhanced EAS
- LG Integrity Monitoring

Mobile Device Management

- LG MDM

Platform Security

Ensure integrity across all software components and provide access control.

Enhanced Secure Boot

- Maintain the integrity of software components at system boot time.
- Strengthen system protection through more secure algorithm and longer key size.
  - Reinforced security key strength for asymmetric key: RSA2048
  - Strong hash algorithm: SHA-256

SE Linux

- Enforce MAC (Mandatory Access Control) policy provided by SE Linux to minimize vulnerability.
  - Prevent privilege escalation of unauthorized apps
  - Prevent data leakage
  - Protect integrity of apps and data
  - Provide a centralized/analyzable policy
  - Improve application isolation/sandboxing
  - Protect from misuse and contain damage of app and service
  - Mitigate risks of flawed and malicious programs
  - Protect from rooting attacks

LG GATE

› Platform Security

Safeguard your corporate data on-device without compromising security or sacrificing performance.

Enhanced Data Encryption

- Strong encryption algorithm (AES-256)
- Satisfying FIPS140-2** (U.S Federal Government Standard)
- APIs available to enforce encryption via device management applications, e.g. MDM apps
- Additional user-friendly features include:
  - Enable/Disable encryption for both internal and SD card storage
  - Optionally exclude media files from encryption
  - Quick encryption

Hardware Accelerated Encryption*

- More secure encryption process than software-based encryption
- Faster and better user experience

* The HW Accelerated Encryption feature is applied on selected models. ** For other models, the FIPS140-2 certified SW crypto module is applied.

LG GATE

Platform Security

Protect the keys used for data encryption and the certificates in Android™ KeyStore using TrustZone (TZ) technology.

Enhanced Key Management

- Encryption keys are protected from malicious attacks by the key derived from Trust Zone.*
- Encryption keys are managed in secure manner compliant to the U.S. Federal Gov. requirement.
    - Key generation with secure key materials
    - All key materials & security parameters are wiped out if no longer needed

TZ-based Certificate Management

- Certificates encrypted by TZ are stored in Android KeyStore for protection.
- TZ manages asymmetric key pairs for certificates.
    - Key generation
    - Import asymmetric keys
    - Signing and verifying authentication codes

* The TZ-based Key Protection feature is applied on selected models.

LG GATE

› Network Security

Stay securely connected with your corporate network.

LG VPN (Virtual Private Network)

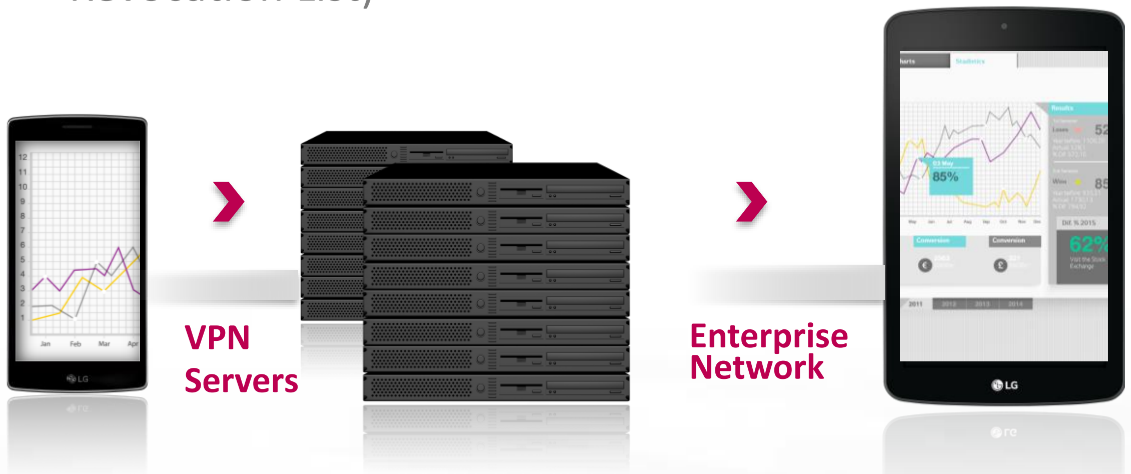
Secure and seamless connection via major VPN protocols to enterprise intranet.

- Meets FIPS140-2 (U.S Federal Gov. Standard)
- Connect with major VPN servers via one device
- Support SSL VPN on top of Android™ native VPN framework
- Accommodate Advanced IPSec VPN through LG VPN solution extension
- Compatible with major VPN gateways

  - CheckPoint, Cisco, Fortinet FortiGate, Juniper, NETGEAR ProSafe, SonicWALL, StrongSwan, ZyXEL, StoneSoft, Windows Server

Enhanced Certificate Validation*

- Robust validation for all certificates to protect your secure connection from spoofing and invalid certificates.
  - ○ Validation using CRL (Certificate Revocation List)



VPN Servers

Enterprise Network

* The Enhanced Certificate Validation feature is activated in CC (Common Criteria) mode on NIAP MDF PP certified devices

LG GATE

› Application Security

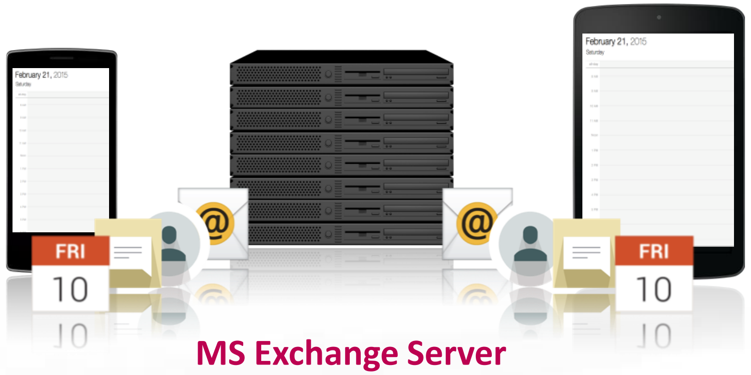
Sync applications so you can securely access work email and content.

Enhanced EAS

Extend the support of Microsoft Exchange ActiveSync policies so you can seamlessly and securely access corporate email while on the go.

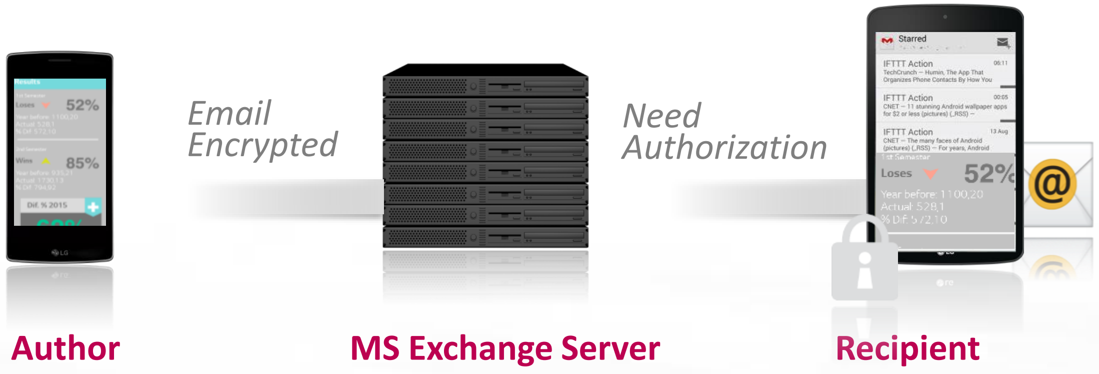
Simple Sync

- Simple Email, Contacts, Calendar, and Tasks syncing among devices



Secure Email

- Recipients can only open, edit, reply, forward, or print the email and contents given the email author's authorization
- S/MIME* and IRM** support



Restrict to Open, Reply, Forward or Print based on Author's authorization

* S/MIME - a security-oriented superset of Multipurpose Internet Mail Extensions (MIME)
** IRM – Information Rights Management (control the rights recipients have for e-mail)

Application Security

Detect and report alteration of your mobile applications.

LG Integrity Monitoring

Prevent malicious attacks by detecting replaced or modified applications. Provide a notice to the application management to take an action to mitigate any security risks.

- Verify the integrity of user applications on device
  - Run-time checking (application execution time)
  - Measurement data securely stored in Trust Zone
  - Strong hash algorithm: SHA-256
- Notify the failure of integrity check to device management applications (e.g. MDM) and user.
- Provide APIs for managing applications and measurement data to device management applications (e.g. MDM)
  - Integrity monitoring service control: enable / disable
  - MDM APIs: install / uninstall, block app execution, etc.
  - Application measurement data management: generate, remove, update

* The LG Integrity Monitoring feature is applied on selected models.

Mobile Device Management

Ensure a secure, reliable way to access work when on the go.

LG MDM (Mobile Device Management)

Provide Security & Manageability of Mobile Devices Remotely.

1. Configuration & Management

- Email/EAS, VPN, Wi-Fi® Configuration
- Application Management
- Security Management

2. Granular Device Control

- Hardware control: BT, Camera, Wi-Fi, Microphone, SD Card, NFC, etc.
- Feature control: Tethering, Screen capture

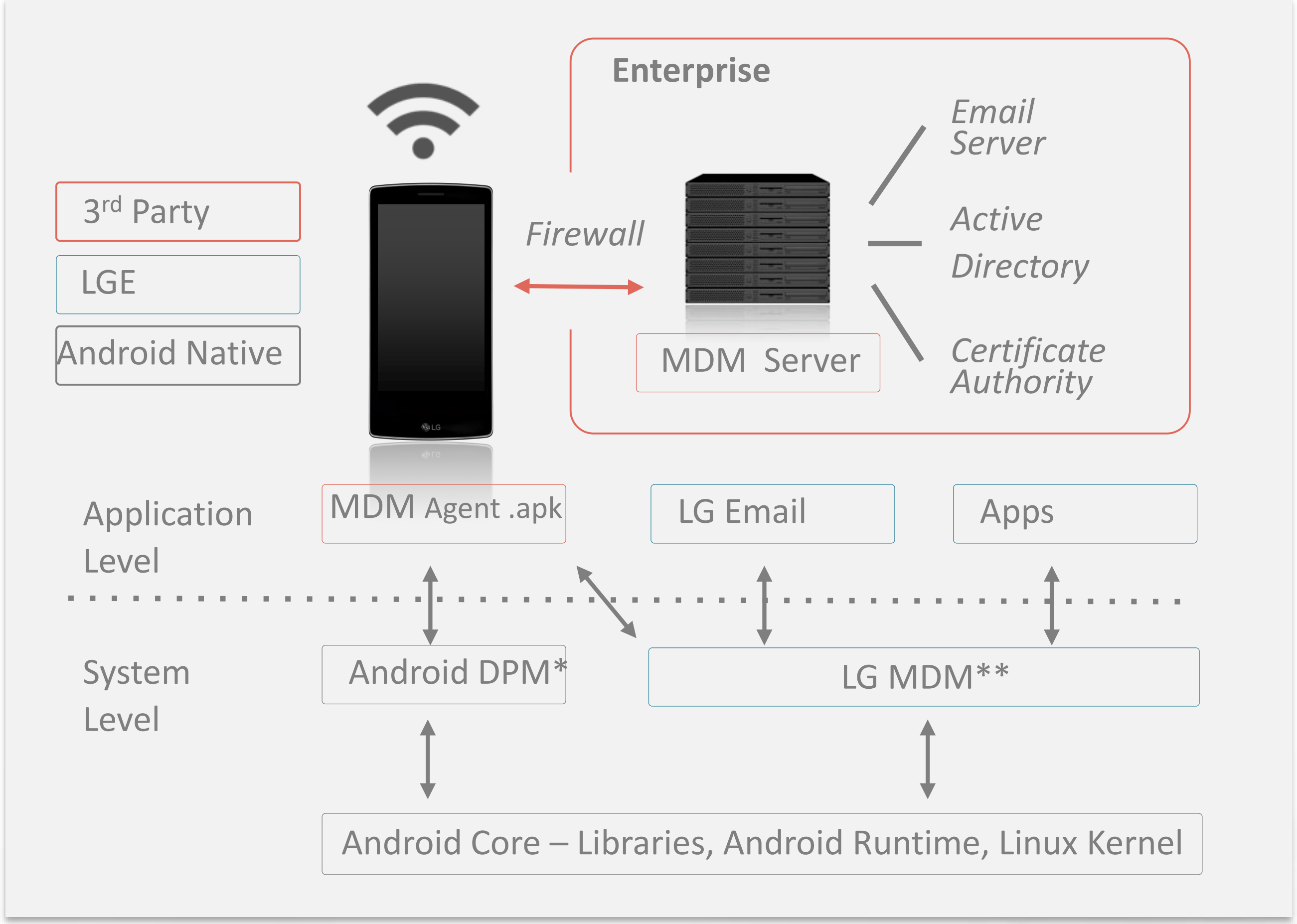
3. Device Protection

- Wipe all data or lock the device when lost
- Strong password policies
- Rooting detection

Mobile Device Management

LG creates extended MDM APIs in Android™ framework so that ISVs can leverage them.

	LG Android	Native Android
Model	G3	Nexus 5
API	356	46
Feature	• Password Policy • Wipe device • Lock device • Require encryption • Allow camera • Allow Wi-Fi® / *Bluetooth®* / NFC / microphone / SD Card / USB, etc. • Allow screen capture • Allow tethering • Allow browser • Allow Google Play™ • Allow YouTube® • Allow clipboard • Allow unknown source • Configure Email / VPN / APN / Certificate •Delete data/cache/default of App • Install / Uninstall App • App Black list / Whitelist • Rooting detection • etc.	• Password Policy • Wipe device • Lock device • Require encryption • Allow camera • etc.



Enterprise

Email Server

Active Directory

Certificate Authority

MDM Server

Firewall

3rd Party

LGE

Android Native

Application Level

MDM Agent .apk

LG Email

Apps

System Level

Android DPM*

LG MDM**

Android Core – Libraries, Android Runtime, Linux Kernel

[*] Android Device Policy Manager has been supported since Android 2.2 (Froyo)

[**] extended LG MDM features can benefit enterprises only if enterprises adopt LG MDM partner's solution

LG GATE

Certifications

Ready for the highly regulated corporate environment and government grade security.

FIPS140-2 Certification

- FIPS (Federal Information Processing Standard) 140-2 Level 1 certification issued by the NIST (National Institute of Standards and Technology).
- Meets the US Government security requirements for Cryptographic Modules of both Data-At-Rest and Data-In-Transit.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIAP MDF PP* Certification

- MDF PP (Mobile Device Fundamentals Protection Profile) certification issued by the NIAP (National Information Assurance Partnership).
- Meets the Common Criteria which is international security standard required by a number of Governments.

NIAP

DISA STIG* Compliance

- STIG (Security Technical Implementation Guides) development guided by the U.S. DISA (Defense Information Systems Agency) and publication.
- Meets the U.S. DoD (Department of Defense) security requirements to deploy mobile devices.

DEFENSE INFORMATION SYSTEMS AGENCY

* The NIAP MDF PP certification and DISA STIG compliance are available for selected models in North America.