TMW01 – Managing and Deploying BYOD Identity Solutions with a Microsoft PKI

Mark B. Cooper
President & Founder
PKI Solutions Inc.

@PKISOLUTIONS

Level: Intermediate
[

LIVE! 360
TECH EVENTS WITH PERSPECTIVE

IT AND DEVELOPER TRAINING THAT'S OUT OF THIS WORLD

Visual Studio LIVE! | SharePoint LIVE! | SQL Server LIVE! | Modern Apps LIVE! | TECHMENTOR

About PKI Solutions Inc.

- **10 years as “The PKI Guy” @ Microsoft**
- **Charter – Microsoft Certified Master DS**
- **Numerous books and whitepapers**
- **Services include:**
  - ADCS Architecture, Deployment and Consulting
  - Assessment and Remediation Services
  - In-Depth PKI Training

    SFO January 2015, NYC February 2015
  - Retainer and Support Services

Agenda

- PKI ecosystem changes
- BYOD and the Internet of Things
- Fundamentals of BYOD
- PKI architecture and requirements
- Microsoft’s BYOD solution
- 3rd party products

PKI ecosystem changes

The ecosystem today

- **PKI adoption rates are quickly increasing**
- **Evolving usage scenarios**
  - Traditional uses
  - Greater product integration and dependencies
- **Scaling and availability**
  - Fault tolerance
  - OCSP
- **Integration into continuity plans**

The ecosystem today

- **Evolving to meet the new enterprise**
  - Disconnected
  - Unmanaged
  - Diverse
  - Computers AND devices

BYOD and the Internet of Things

Adopting BYOD

- **BYOD and corporate security policies**
  - 180 degree change from traditional models
  - Primarily user driven demand
- **Accessibility**
  - What’s the cost?
  - Risk versus reward
- **Affects security postures**
  - BYOD S/Mime & Smart cards
  - Weaknesses will be exploited

The Enterprise and the Internet of Things

- **IoT evolving**
  - Tighter interaction with corporate networks
  - De-evolution of PSTN and side-band communications
- **IoT challenges everything**
  - Integrated OSes
    - **Management**
    - **Security**
    - **Identity**
- **Shell Bash**
  - – Weaknesses will be exploited

Fundamentals of BYOD

Management Goals

- **Desire to manage information and access**
  - Data partitioning and centralize management
  - Corporate information access and rights
- **Manage anything anywhere**
  - Centralized management and accounting
  - Centralized mitigation and exposure control
- **“The device is the new desktop”**

Diverse platforms

- **Organizations inherently want to organize**
  - Challenges of disparate platforms and capabilities
  - Desire for uniformity and user experience
- **Management dependent on ownership**
  - Explicit ownership
  - Implicit management privilege

Devices need access

- **Requirements**
  - Wired/Wireless network access
  - Remote Desktop Services
  - VPN and other tunnels (Direct Access)
  - Consumable applications and services
- **Considerations**
  - Access technology is the easy part
  - Most devices have the capability
  - Dependent on organization identities and access controls
  - Ability to consume and use identity proof is the unknown

Devices need identities

- **Requirements**
  - Establishes the who or what for the device
  - Deterministic attribute for access controls
  - Enables centralized identification of device
- **Considerations**
  - Lack identities you can trust or leverage out of the box
  - Needs an identity in your environment
    - **User identity**
    - **Device identity**
  - Value of unique identities
  - Assured with Client Authentication certificate

Devices need protection

- **Requirements**
  - Information encryption
  - Device security and assurance
  - Remote lock and/or wipe
  - Location services
- **Considerations**
  - Information protection dependent on ability to secure it
  - Centralized security settings and enforcement
  - Information encryption
  - May require encryption enable certificate

PKI architecture and requirements

Devices need access

- **Requirements**
  - Wired/Wireless network access
  - Remote Desktop Services
  - VPN and other tunnels (Direct Access)
  - Consumable applications and services
- **Considerations**
  - Access technology is the easy part
  - Most devices have the capability
  - Dependent on organization identities and access controls
  - Ability to consume and use identity proof is the unknown

BYOD & PKI integration

- **Trust**
  - Generally handled by the BYOD solution
  - Provided in provisioning
  - Provided in PKCS7b chain file
- **CDP & AIA**
  - Most critical component to successful PKI
  - Accessible to BYOD/IofT devices
  - **HTTP is only true option**
  - Not easy to modify down the road
  - Designs allow for name flexibility for future needs

BYOD & PKI integration

- **Enrollment**
  - BYOD not part of managed environment
  - Manual options
  - The true benefit of BYOD solutions
  - RPC/DCOM native enrollment
  - CES/CEP proxied enrollment
  - NDES integrations
  - **Historical OTP enrollment issues**

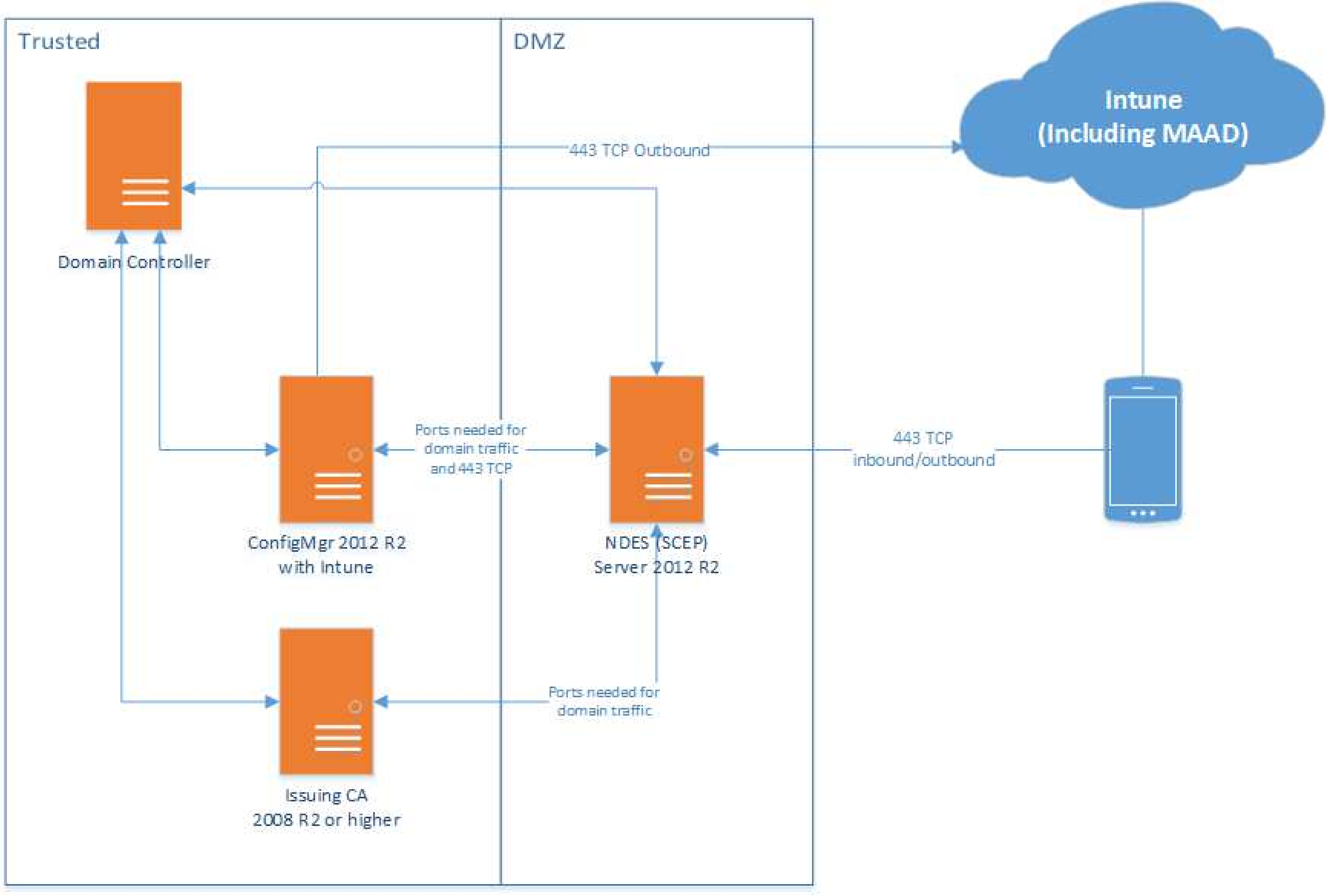
Microsoft’s BYOD solution

Microsoft Intune

- **Formerly Windows Intune**
  - Originally designed for non-traditional PC management
  - SCCM “like” for the unmanaged environment
- **Expanded to fit BYOD scenarios**
  - Supports variety of client bases and platforms
    - **Windows, iOS, Android**
  - Provides ability to manage the unmanageable
  - Integrates with infrastructure systems

Intune components

- Cloud based Intune service
- Local SCCM environment
- *NEW* Server 2012 R2 NDES Policy Module
  - Offloaded Authentication and Enrollment Management
  - Authorization Tied to Enrollment Request
- New Whitepaper From Microsoft



Trusted

DMZ

Intune (Including MAAD)

443 TCP Outbound

Domain Controller

Ports needed for domain traffic and 443 TCP

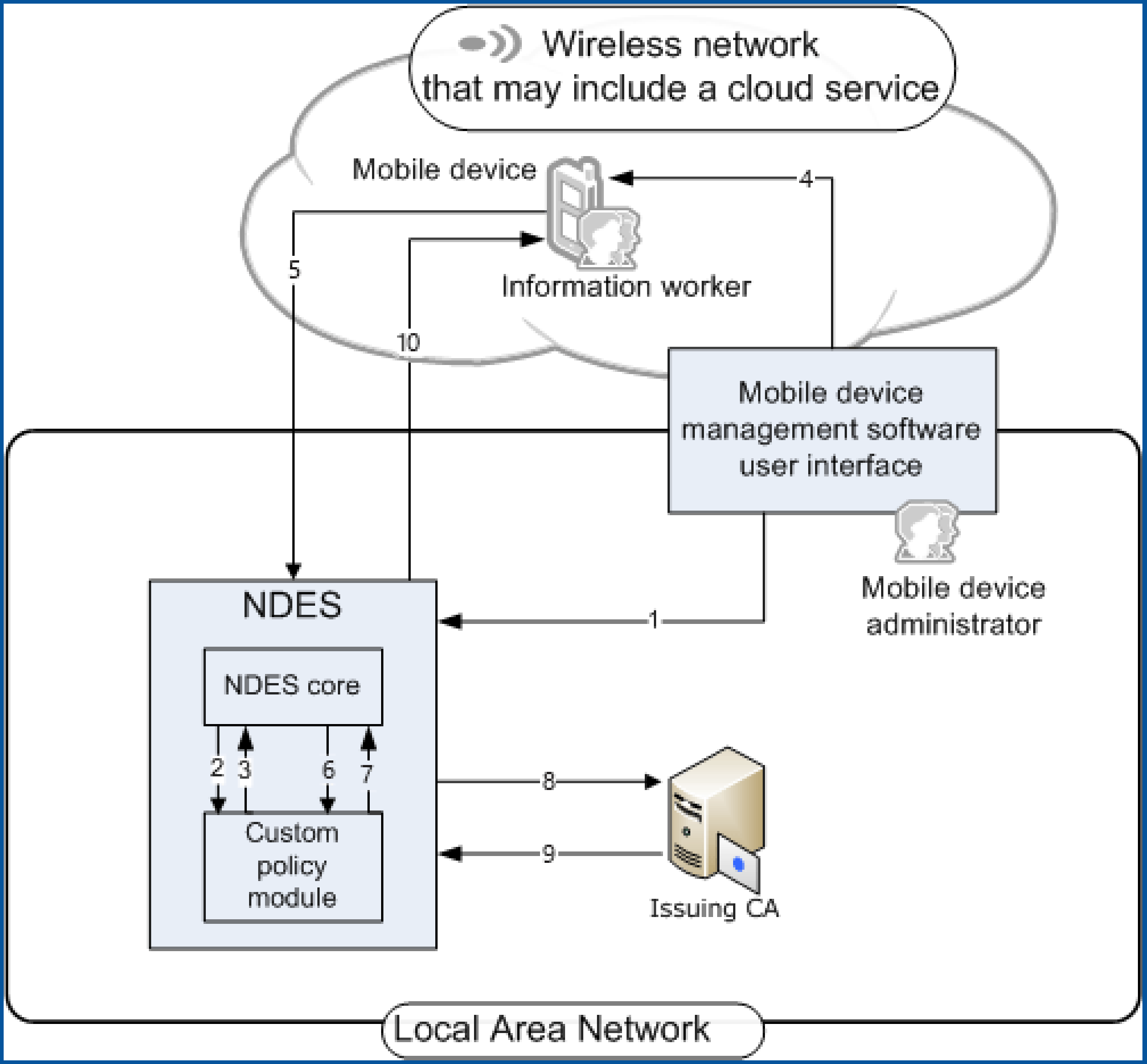
ConfigMgr 2012 R2 with Intune

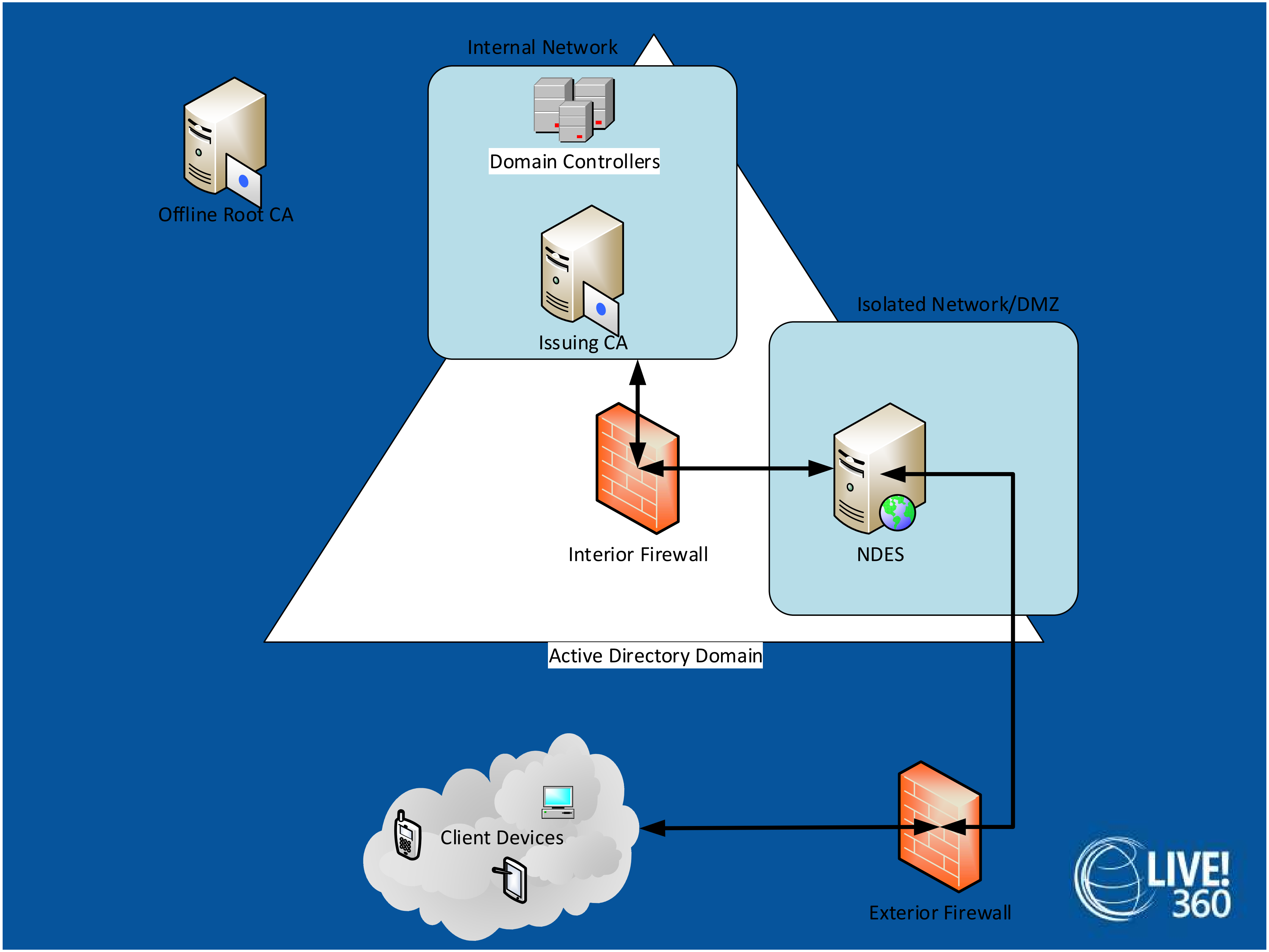
NDES (SCEP) Server 2012 R2

443 TCP inbound/outbound

Ports needed for domain traffic

Issuing CA 2008 R2 or higher


Wireless network
that may include a cloud service
Mobile device
Information worker
4
5
10
Mobile device
management software
user interface
Mobile device
administrator
NDES
1
NDES core
2
3
6
7
Custom
policy
module
8
9
Issuing CA
Local Area Network


Offline Root CA
Internal Network
Domain Controllers
Issuing CA
Isolated Network/DMZ
Interior Firewall
NDES
Active Directory Domain
Client Devices
Exterior Firewall

3rd party solutions

Busy marketplace

- Abundance of providers
- Historical gap in enterprise management
- Leveraged infrastructure and extended to BYOD
- Cloud and premises solutions
- Hybrid options
- Integrate with corporate PKIs

airwatch

MobileIron

Solution considerations

- Identity management
- Issuance and revocation
- Integration with existing PKI
- Signing key management and security

Questions?

pkisolutions.com

mark@pkisolutions.com

@pkisolutions

Next Session

Securing Cloud Servers and Services with PKI Certificates