National Cybersecurity Center of Excellence

Derived Personal Identity Verification (PIV) Credentials

Federal Computer Security Managers Forum

November 2, 2017

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

ABOUT THE NCCOE

Mission

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

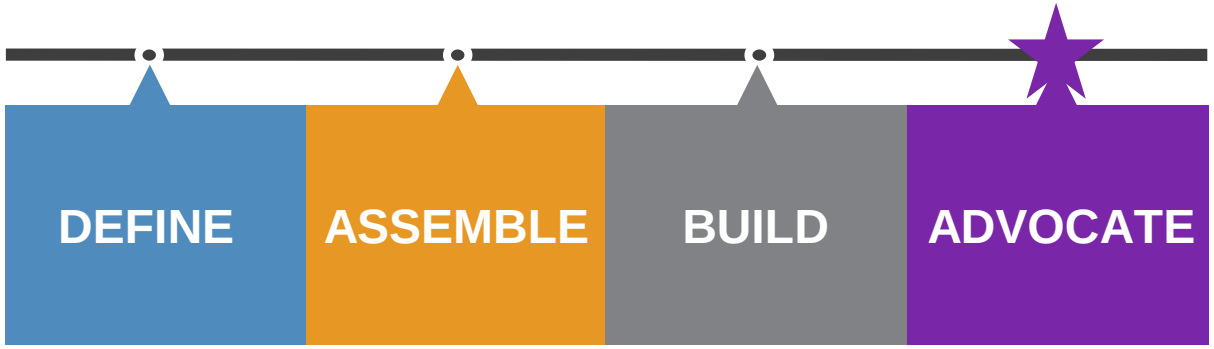
DERIVED PIV CREDENTIALS

Derived PIV Credentials

An alternative token: direct implementation and deployment

Overview

- Tablets and mobile phones do not have smart/PIV card readers, which means Federal users of those devices are unable to leverage the PIV Card
- This project builds upon NISTIR 8055, a proof-of-concept prototype platform for use of Derived PIV Credentials in a mobile environment
- This project will demonstrate the lifecycle of Derived PIV Credentials as described in SP 800-157



Project Status

Accepting public comments on SP 1800-12 Practice Guide draft.

Collaborate with Us

- Read Derived Personal Identity Verification (PIV) Credentials Practice Guide and submit comments
- Email piv-nccoe@nist.gov to join the Community of Interest for this project

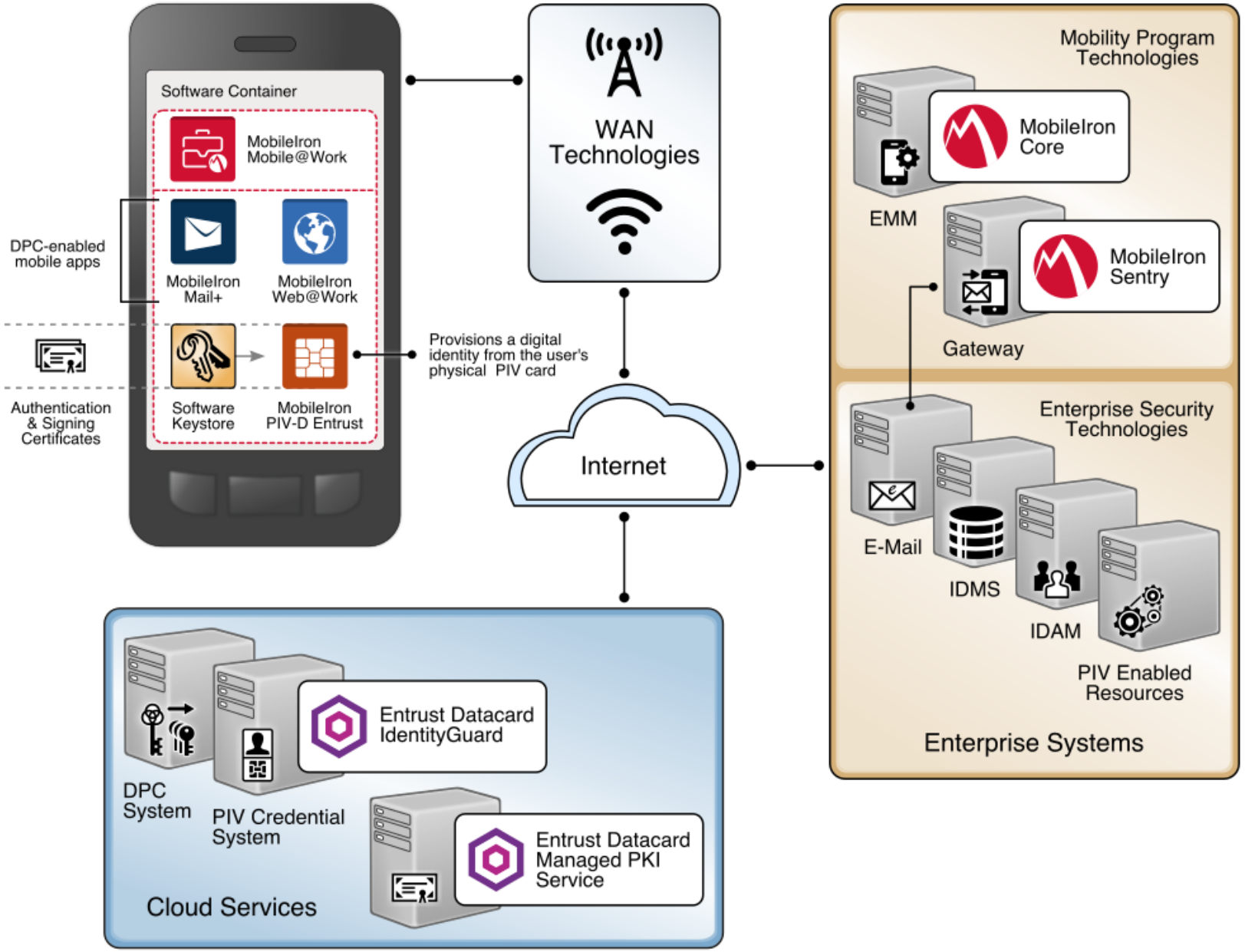
Derived PIV Credentials: Potential Outcomes

Adopting all or part of the example implementation can:

- Provide strong multifactor authentication to PIV enabled web sites, eliminating reliance on less secure authentication methods such as passwords
- Provide cost savings by incorporating the user's previously established PIV identity into the new Derived PIV Credential, thereby eliminating the need for further identity proofing
- Provide seamless integration of Derived PIV Credential issuance with Enterprise Mobility Management (EMM) systems

- Engagement with Federal Agencies on their efforts with DPC
  - Lessons learned from pilots and implementations as input to SP 800-157
  - Collaboration with GSA to expand the user interfaces to Shared Service Providers to include support for DPC
- Collaboration among COTS vendors to build example implementations that follow the 800-157 guidelines and promote standard interfaces
- Publication of practice guide Special Publication 1800-12

DERIVED PIV MANAGEMENT VIA CLOUD + EMM



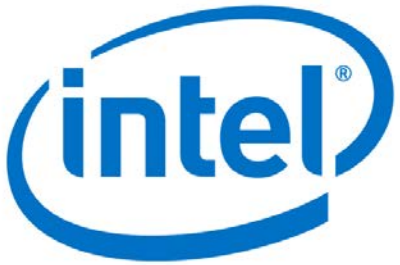

Entrust Datacard™


MobileIron


intercede

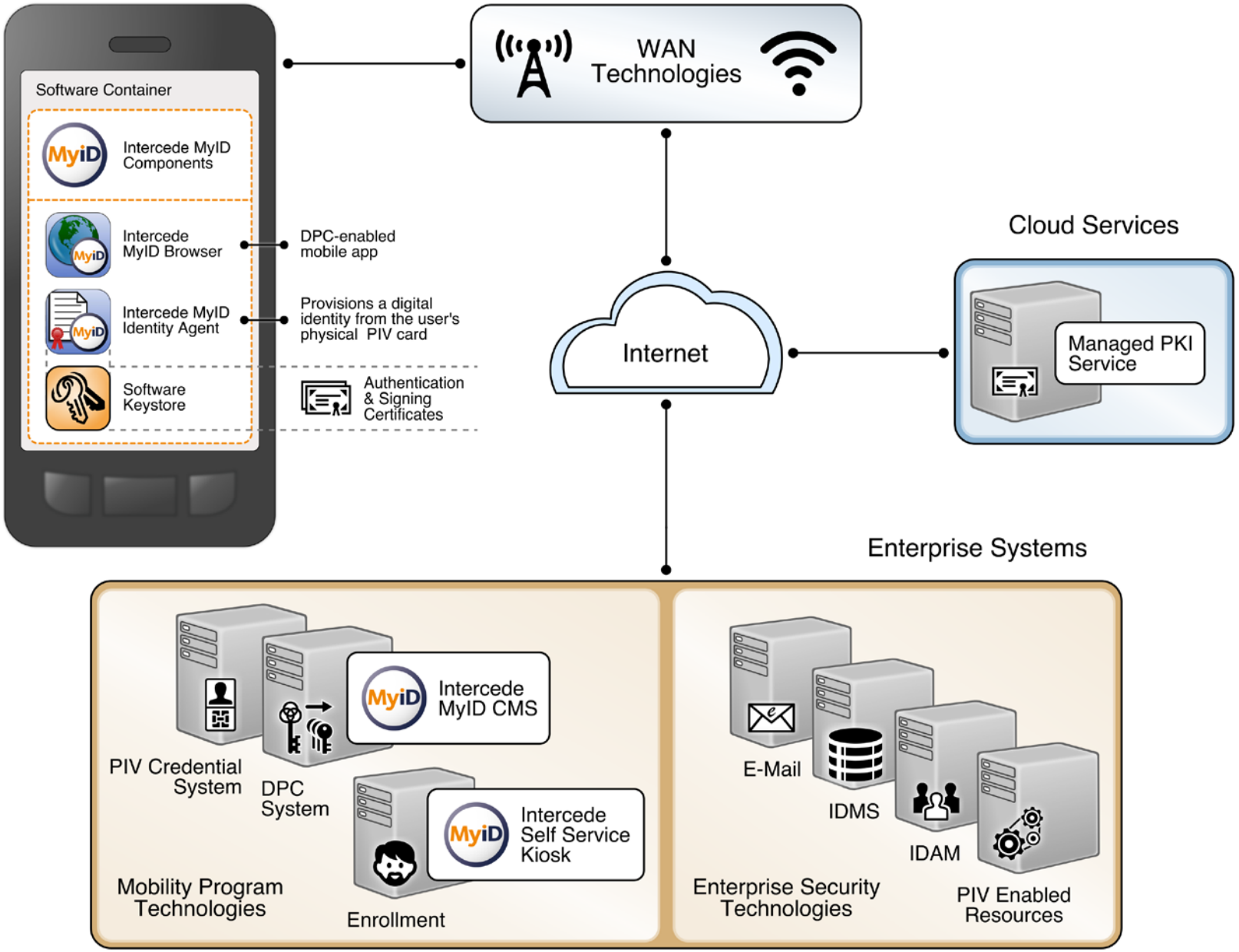

vmware®


IBM®

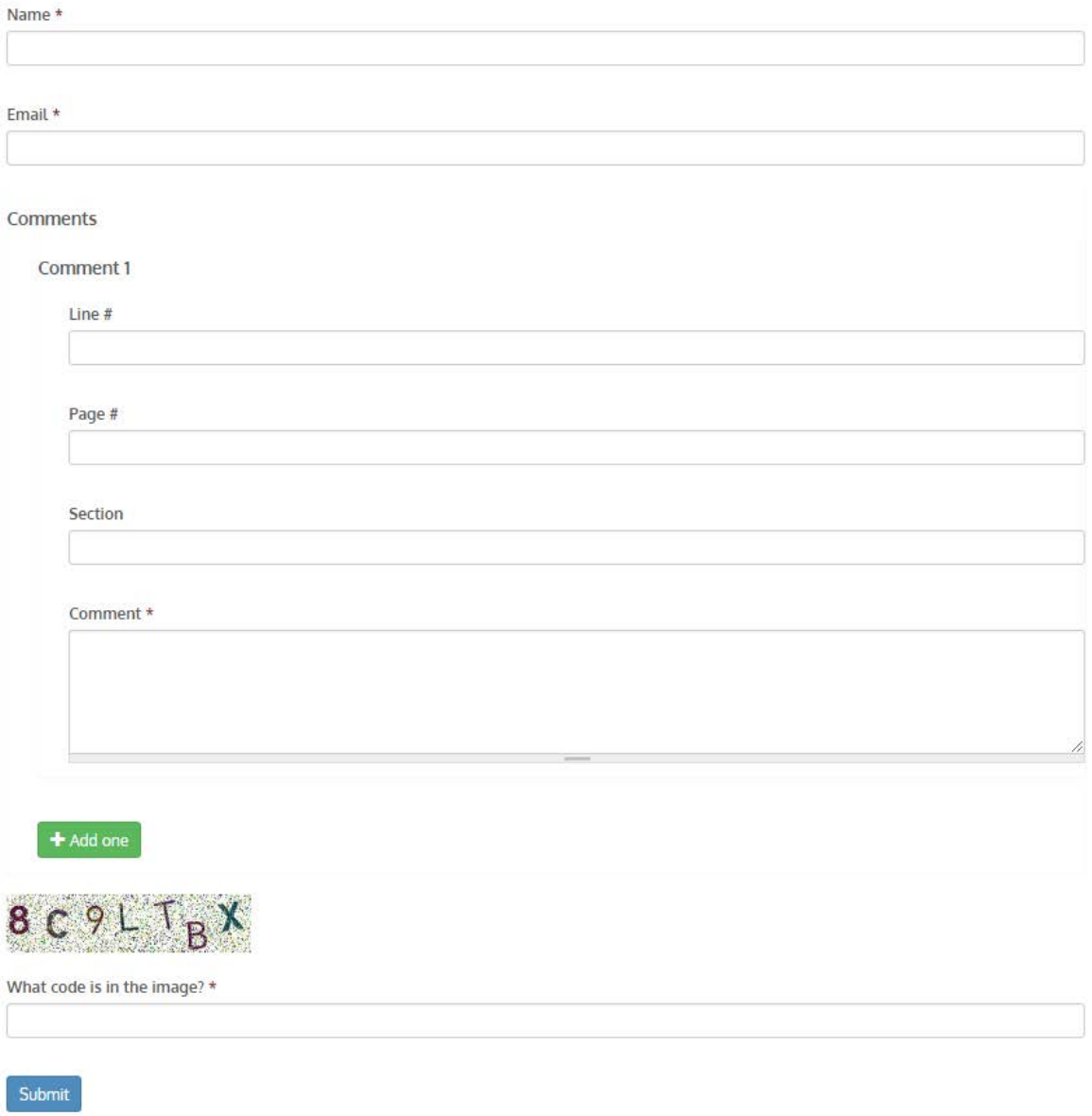

intel®


Route1®

ON PREMISE DCMS + CLOUD PKI MANAGED SERVICE



SUBMIT COMMENTS ON SP1800-12



https://nccoe.nist.gov/webform/comments-sp-1800-12-derived-piv-credentials

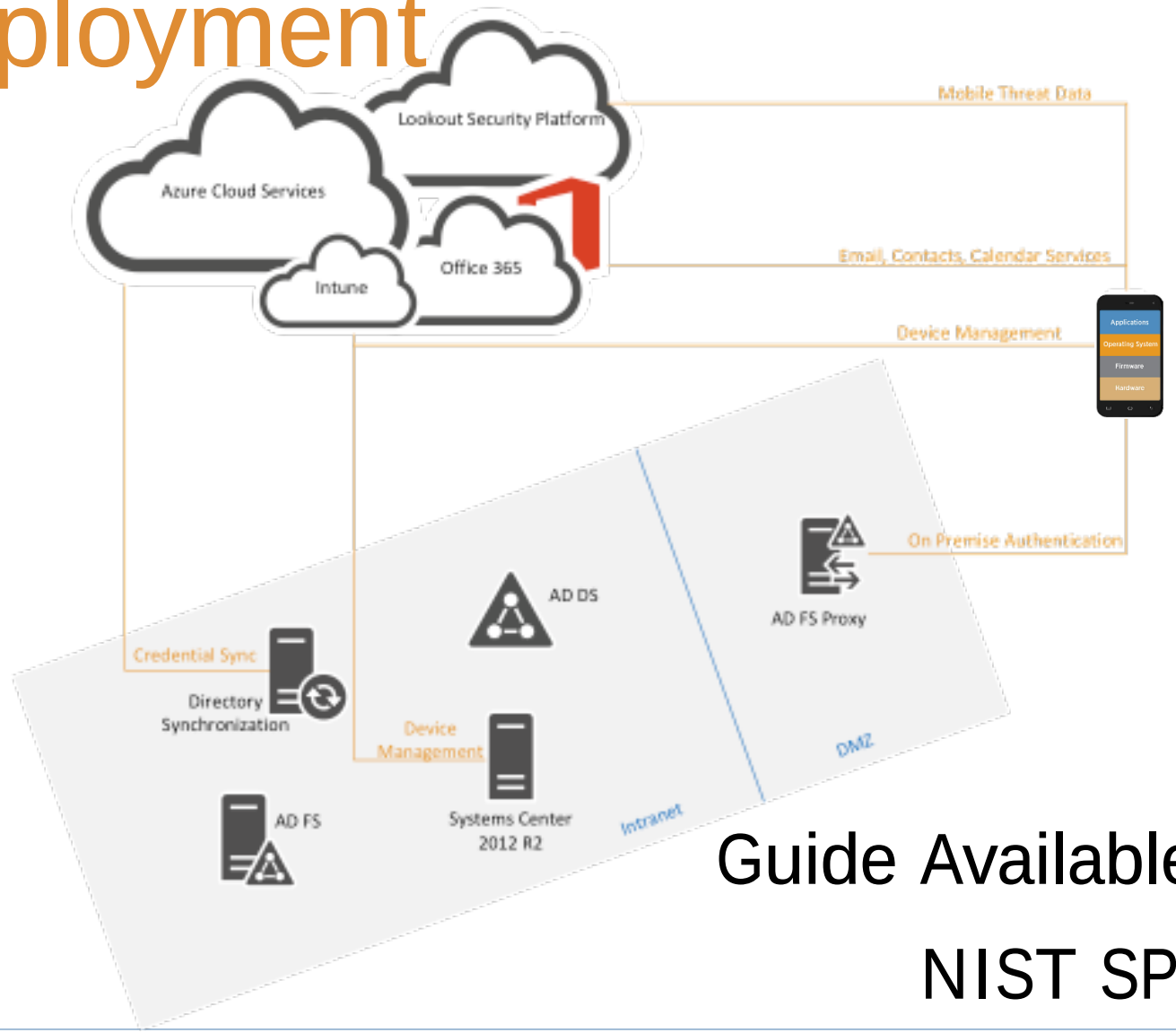
MOBILE DEVICE SECURITY

Build Goals

Demonstrate commercially available mobility management technologies:

- **Securely enable basic email, calendar and contacts**
- Allowing for granular control over the enterprise network boundary
- Minimizing the impact on function

Deployment



Guide Available Online

NIST SP 1800-4

Public Response to SP 1800-4

- Many respondents highlighted a need for a more robust threat model
- Additional risks and mitigations were provided
- User education was highlighted as a missing factor
- Demonstrate use of the NIST Cybersecurity Framework
- Need a full treatment of privacy
- Include Blackberry

Mobile Threat Catalogue

- Identify threats to devices, applications, networks, & infrastructure
- Collect countermeasures that IT security engineers can deploy to mitigate threats
- Inform risk assessments
- Build threat models
- Enumerate attack surface for enterprise mobile systems
- Assist in standards mapping activities

Collected Information Per Threat

- **Threat Category:** The major topic area pertaining to this threat. Topic areas are further divided when necessary.
- **Threat Origin:** Reference to the source material used to initially identify the threat.
- **Exploit Example:** References to specific instances of this threat.
- **Common Vulnerability and Exposure (CVE) Reference:** A specific vulnerability located within the National Vulnerability Database (NVD).
- **Countermeasure:** Security controls or mitigations identified to reduce the impact of a particular threat.
- **References**: Links to talks, publications, and academic papers.

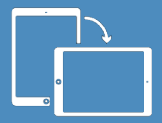
HIGH LEVEL CATEGORIES

APPLICATION
Mobile applications

AUTHENTICATION
Something you know, have, or are

CELLULAR
Telecommunications networks

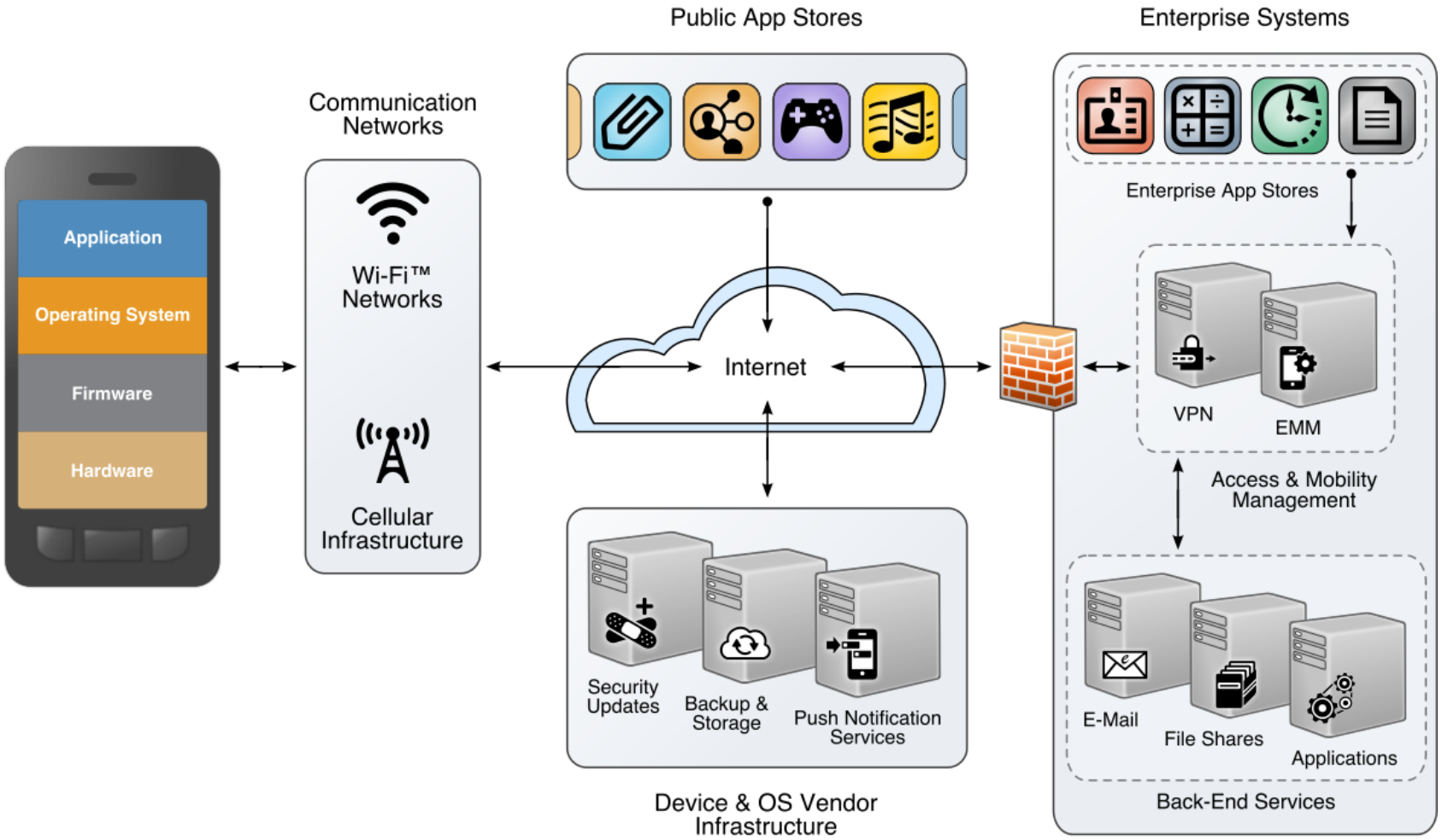
ECOSYSTEM
Vendor infrastructure, application stores



MOBILE DEVICE
Hardware, firmware, OS

NETWORK INTERFACES
Wifi, NFC, Bluetooth

HIGH LEVEL CATEGORIES



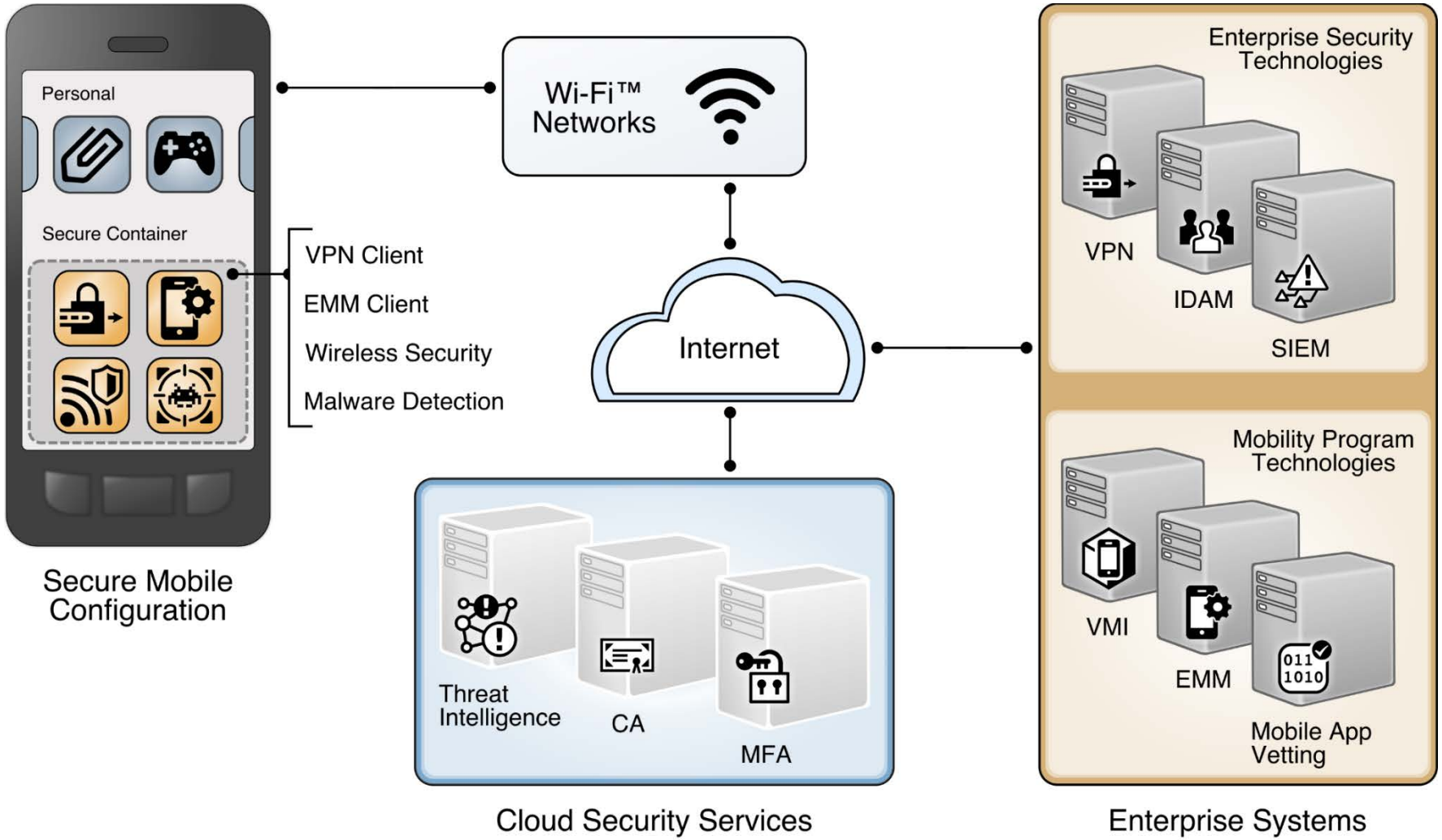
MOBILE DEVICE SECURITY FOR ENTERPRISES

Continuation of SP 1800-4

- Other ways exist to solve the original MDS problem statement
- Creating 2 new builds to show different methods
- Using the same problem definition from 2014

MDSE Builds

- ***Government Build*** – strong data confidentiality is implemented using federally certified and validated technologies
- ***Enterprise Build*** – business productivity tools are deployed alongside a variety device policies for employees with different risk profiles


Personal
Secure Container
VPN Client
EMM Client
Wireless Security
Malware Detection
Secure Mobile Configuration
Wi-Fi™ Networks
Internet
Threat Intelligence
CA
MFA
Cloud Security Services
Enterprise Security Technologies
VPN
IDAM
SIEM
Mobility Program Technologies
VMI
EMM
011 1010
Mobile App Vetting
Enterprise Systems

EMAIL: piv-nccoe@nist.gov

WEBSITE: nccoe.nist.gov

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE