Testing the Public Key Infrastructure

An automated and modularized approach

Stephen Corlett
May 2014
ITEA Workshop, Las Vegas NV

© 2014 TASC, Inc.

TASC
INSIGHT APPLIED

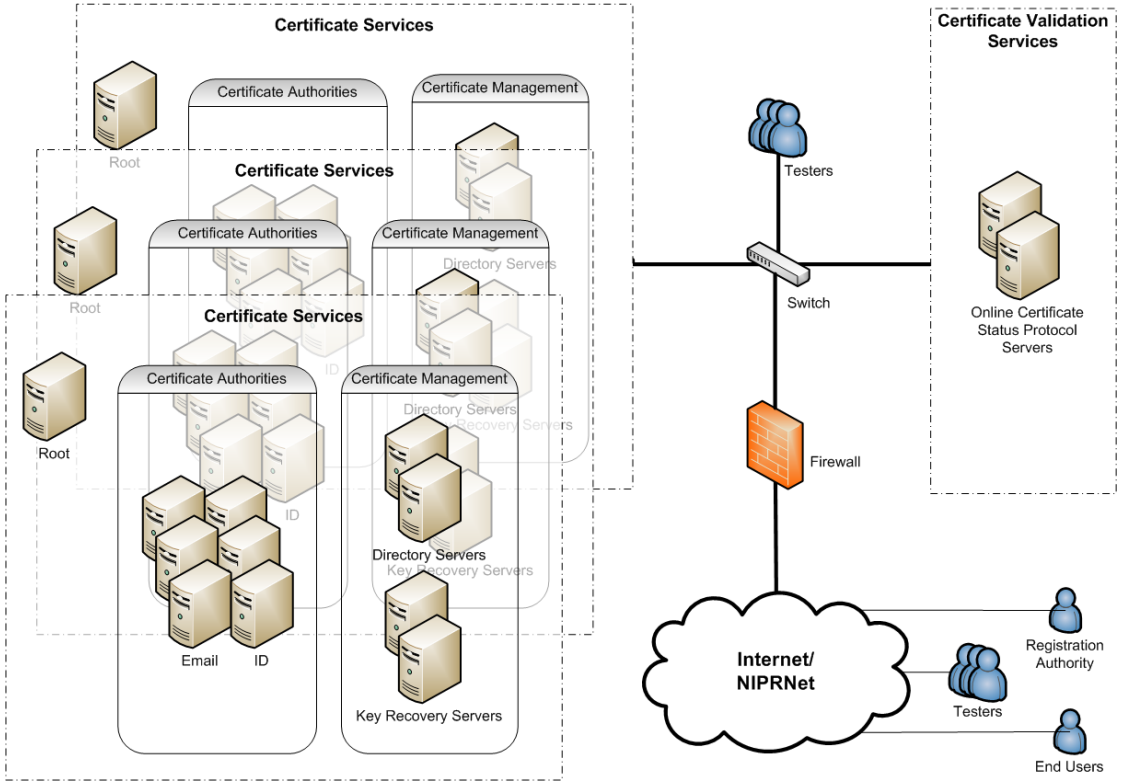
Discussion

- Current state
- Test methods
- Test system design and implementation
- End state

© 2012 TASC, Inc.

Current State

- Growing enclave of systems
  - Multiple certificate issuance servers staged over time
  - Support systems manage certificate lifecycle
  - Systems manage certificate validation



© 2012 TASC, Inc.

Current State – Testing Methodologies

- Manual test of system:
  - Introduction of new equipment – major releases
  - Ad hoc and at direction of Program Management Office (PMO)
  - Daily/weekly Configuration Management (CM) changes
- Existing tools
  - In-house applications and scripts
  - Largely manual execution
- Untapped tools
  - Open source System Monitoring Server (SMS)

© 2012 TASC, Inc.

Test Methods – Understanding Monitoring Systems

- The SMS
  - Common core of scripts/applications
  - Uses object definition model
    - Defined as all elements needed to perform monitoring on a system
    - Defined using internal configuration and template files
    - Highly configurable
  - Uses built-in CGIs and user customizable scripts
    - PKI uses previously developed scripts and develops new
    - Look at limited return states (with definition):
      - 0 = OK
      - 1 = Warning
      - 2 = Critical
      - 3 = Unknown
  - Can use agents on object systems
  - Scripts run on automated, time-based schedule; require manual execution for special run.

© 2012 TASC, Inc.

Test Methods – Plugin Techniques

- Multiple script and high level languages: Perl, C, and shell based Application Programming Interface (API)
- Exit codes must adhere to API (0-3 w/description)
- Exits codes can mean anything the developer wants
  - A “1” could mean “service generated product but not within specified time requirement.”
- Existing scripts also contain logging functions
  - Scripts that exist perform logging of results for later reporting
  - Scripts easily modified to integrate with SMS functions
  - Use the SMS dashboard for immediate results/state; log results for more detailed reports.
- Full interface test and monitor
  - Code to exercise all elements of web-based user interface
  - Each step logged; final result reported to the SMS as state

© 2012 TASC, Inc.

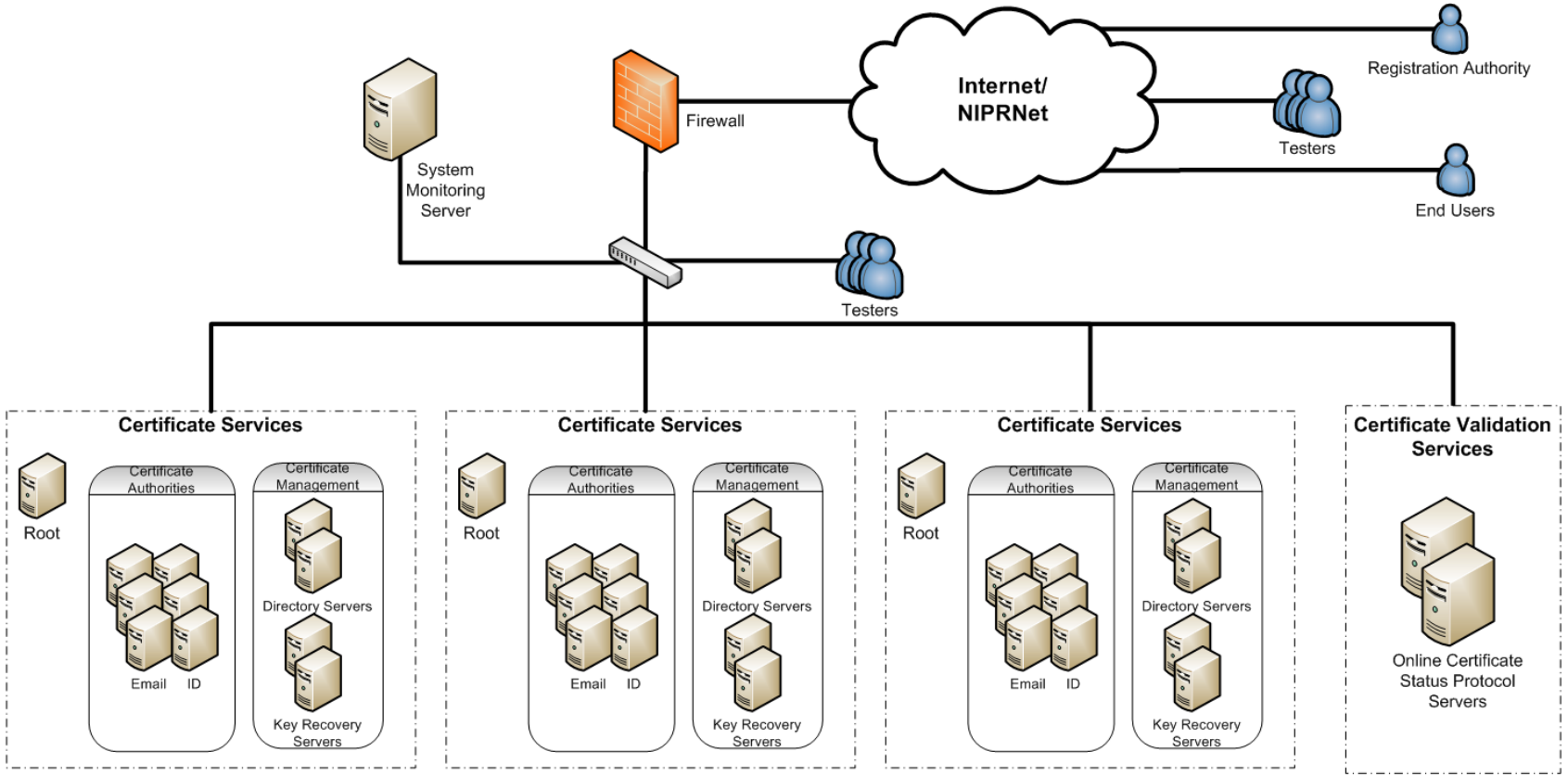
Test Methods – Objects to Test Matrix

- Scripts are reusable throughout enclave
  - Certificate request, search, retrieval, key recovery, and other services common
  - Based on common interface and product delivery
- Configuration and object definition define script usage
  - Commands can execute scripts consecutively or in parallel
  - Commands pass configuration and definition information to scripts

\ Object Script \	CA (w/services)	Key Recovery (w/services)	Directory Server	OCSP
Search	X	X		
CRL retrieval				X
Key recovery		X	X	
Certificate request/ retrieval	X	X	X	

© 2012 TASC, Inc.

Test System Design and Implementation



© 2012 TASC, Inc.

End State

- SMS connected to all objects to be tested
- Modularity - Scripts reusable based on configuration and definitions
  - Report via SMS API and logging structure
  - Additional non-API scripts gather and report on logged data
- Scripts run via timed schedule and report state to the SMS dashboard
- Script collection able to be executed ad hoc via command line
- Provides answer to three testing needs:
  - Major release (partial – must consider external involvement)
  - Ad hoc and PMO requested
  - CM activity baselining

© 2012 TASC, Inc.


TASC
INSIGHT APPLIED

References

- EE Times. Public Key Infrastructure Overview | EE Times. (n.d.). *EE Times*. Retrieved May 5, 2014, from http://www.eetimes.com/document.asp?doc_id=1275792

© 2012 TASC, Inc.