Tumbleweed®

PKI IMPLEMENTATION WORKSHOP
PD-VAL Implementation Recommendations
NIST
April 10-11,2006

Steve Ebbets

Senior Systems Engineer

Tumbleweed Communications

Agenda

Tumbleweed®

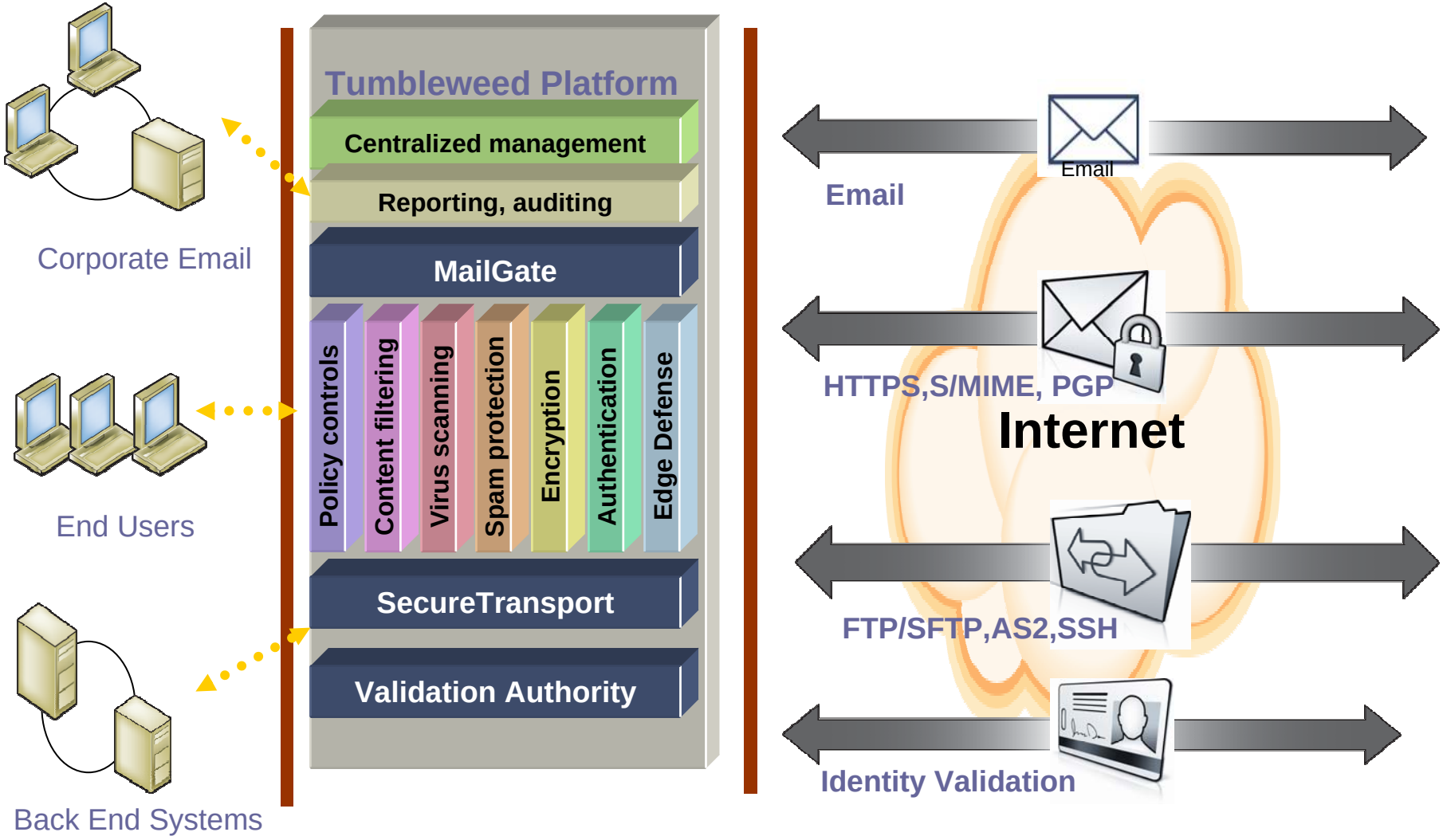
- Overview of Tumbleweed
- Business requirements for PDVAL
- Current Solution
- PDVAL Lessons Learned and Issues
- Deployment Checklist

Company Overview

Tumbleweed®

- **Founded in 1993**
- **Headquartered in Redwood City, CA**
  - Global Presence
  - Global support policy
  - Currently over 300 employees worldwide
  - Publicly traded (NASDAQ:TMWD)
  - Tumbleweed and Valicert merged in June 2003
  - 1500+ Enterprise Customers with over 5 million users
    - Primary focus on Government, Financial and Healthcare
  - 5th & 6th generation of products

Platform Approach



Key Federal Customers

Tumbleweed®

Certificate Validation

- Air Force
- Army ISEC
- Army PM SET-D
- Army CERDEC
- Coast Guard
- DFAS
- DIA
- DISA
- DISA eBusiness (WAWF)
- DLA
- DMS
- DOJ
- Joint Strike Force
- National Geospatial
- NAVAIR
- NAVSUP
- NMCI
- OSD – DMDC
- SPAWAR
- USMC
- WHCA

Email Security

Air Force:
- Eglin AFB
- Wright Patterson AFB
- Kirtland AFB
- Lackland AFB
- Air Force Intelligence

Army:
- Army Rock Island
- Classified Sites (Raytheon)
- Army in Iraq

- Bureau Engraving &Printing
- Department of Energy
- FDA – CDER/CBER/CDRH
- GSA
- HHS
- Intelligence Community
- NRC
- Naval Shipyard
- SPAWAR
- USDA

Secure File Transfer

- Bureau of Public Debt
- Dept of Energy
- DFAS
- EOP
- Federal Reserve System
- GSA
- IRS
- National Business Center
- Naval Crane
- NAVSEA
- OMB
- US Postal Service
- US Treasury
- USMC
- USPTO

Digital certificate validation: Business problem

Tumbleweed®

- **E-Gov applications** rely on their Public Key Infrastructure (PKI) and digital certificates to secure everything from network access to multi-million dollar electronic transactions.
  - **Trusting an invalid or revoked digital certificate can expose an organization to potential fraud, theft, and compromise.**
    - Digital certificate validation enables organizations to maximize their return on investment by ensuring their PKI safeguards all their secure applications.
  - **Certificate Revocation Lists (CRL)**
    - Over time CRLs grow large in size
    - The OCSP and SCVP protocols are always small
  - **Increased complexity with CRL management/distribution across multiple PKIs**.
    - Use of digital certificates in support of HSPD 12 PIV cards will increase this complexity
    - How does Agency A with trust anchor TA validate a certificate from Agency B with trust anchor TB

Tumbleweed®

- **Revocation Status Checking Methods**
  - Certificate Revocation Lists (CRL)
    - Reliance on large CRLs creates many problems:
      - network bandwidth limitations issues with availability,
      - time it takes to download the CRL information from multiple sources
      - inflexibility of handling expired CRLs that are CA signed
    - Need to periodically update
  - On-Line Certificate Status Protocol (OCSP)
    - Certificate trust built by client
    - Trusted roots known
    - Revocation check request sent
  - Simple Certificate Validation Protocol (SCVP)
    - Off loads processing from client
    - Trusted root not known by client
    - Better fit for PDVAL requirements
    - Still a draft

Digital certificate validation: Business problem

Tumbleweed®

- **The government created the Federal Bridge Certificate Authority (FBCA) to**
  - provide an environment in which Federal agencies can request and perform cross-certification with other PKIs
  - allow bridge participants to recognize and trust certificates from other participating organizations.
- **Path Validation**
  - determine the validity and status of these trust relationships
  - locating the correct certificate chains of trust
- **NIST's Public Key Interoperability Test Suite (PKITS) and Path Discovery Test Suite**
  - To ensure compatibility and interoperability of solutions within the FBCA
  - To evaluate and qualify certificate validation solutions

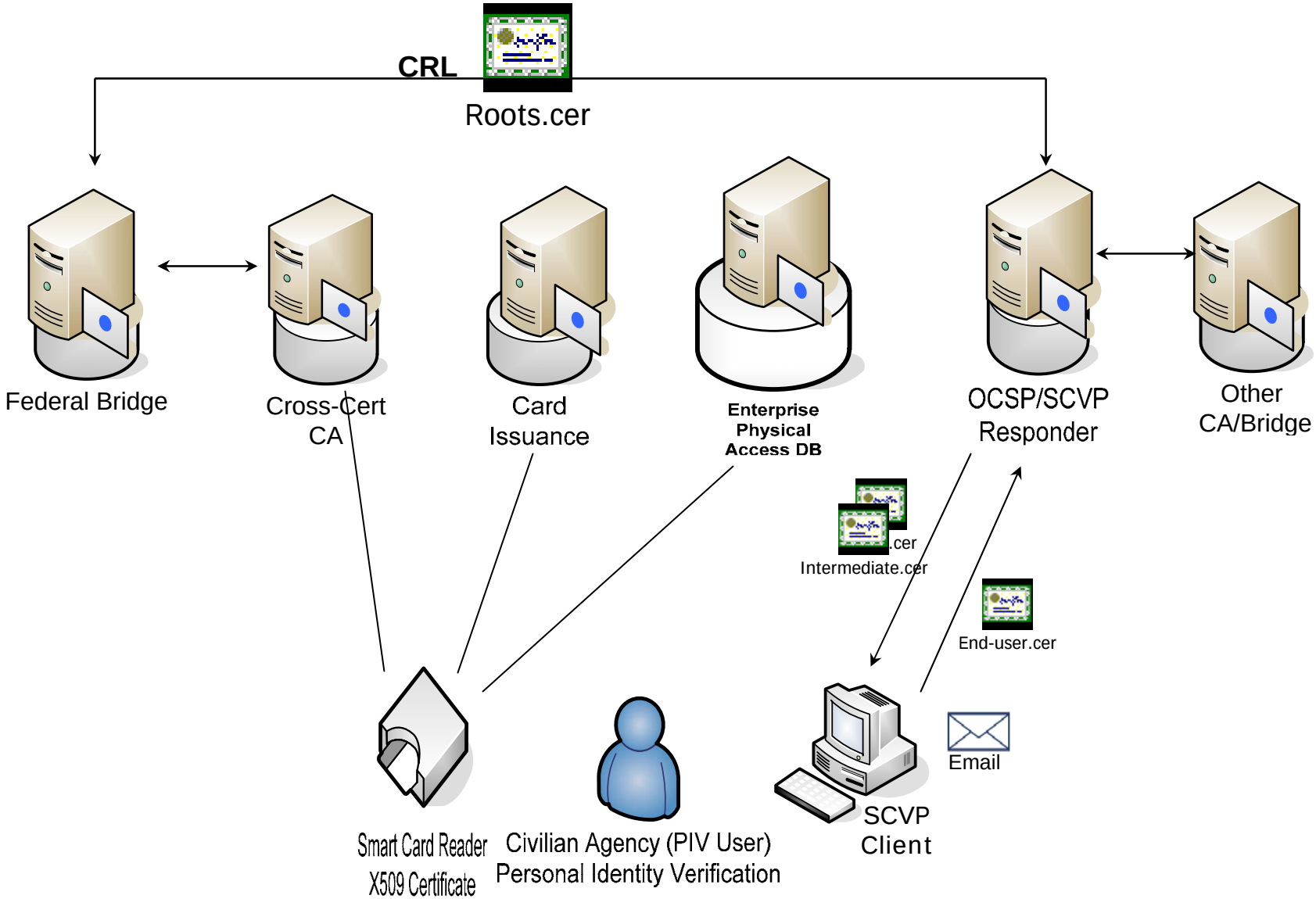
Digital certificate validation: Business problem

Tumbleweed®

- Applications will have perform its own path discovery and validation locally.
  - **Auditing is performed by each PKI-enabled application or by component that performs path discovery and validation.**
- An application may offload these responsibilities to a trusted server.
  - **Delegated Path Validation (DPV) server performs the path validation, path discovery, and most audit functions.**
- The Federal PKI allows for two different approaches to certificate and CRL distribution.
  - **A well-connected directory system**
  - **Certificate contains retrieval information**

HSPD12 and PDVAL

Tumbleweed®



Tumbleweed Solution – Validation Authority

Tumbleweed®

- Validation Authority Server provides a Delegated Path Discovery functionality
  - **Responsible for path discovery, validation, and revocation checking**
  - **PDVAL TWG Qualified Vendor's List**
- Ability to look up CRLdp and AIA - without needing the clients to do so.
  - **Simplifies client**
  - **Improves performance**
- Can return the entire chain to the client and cache discovered certs/CRLs
- Ability to require/ignore certificate extensions in path building gives users the ability to circumvent issues if certificates are minted incorrectly.
- Provides an advantage of centralized auditing

Tumbleweed Solution - Desktop Validator

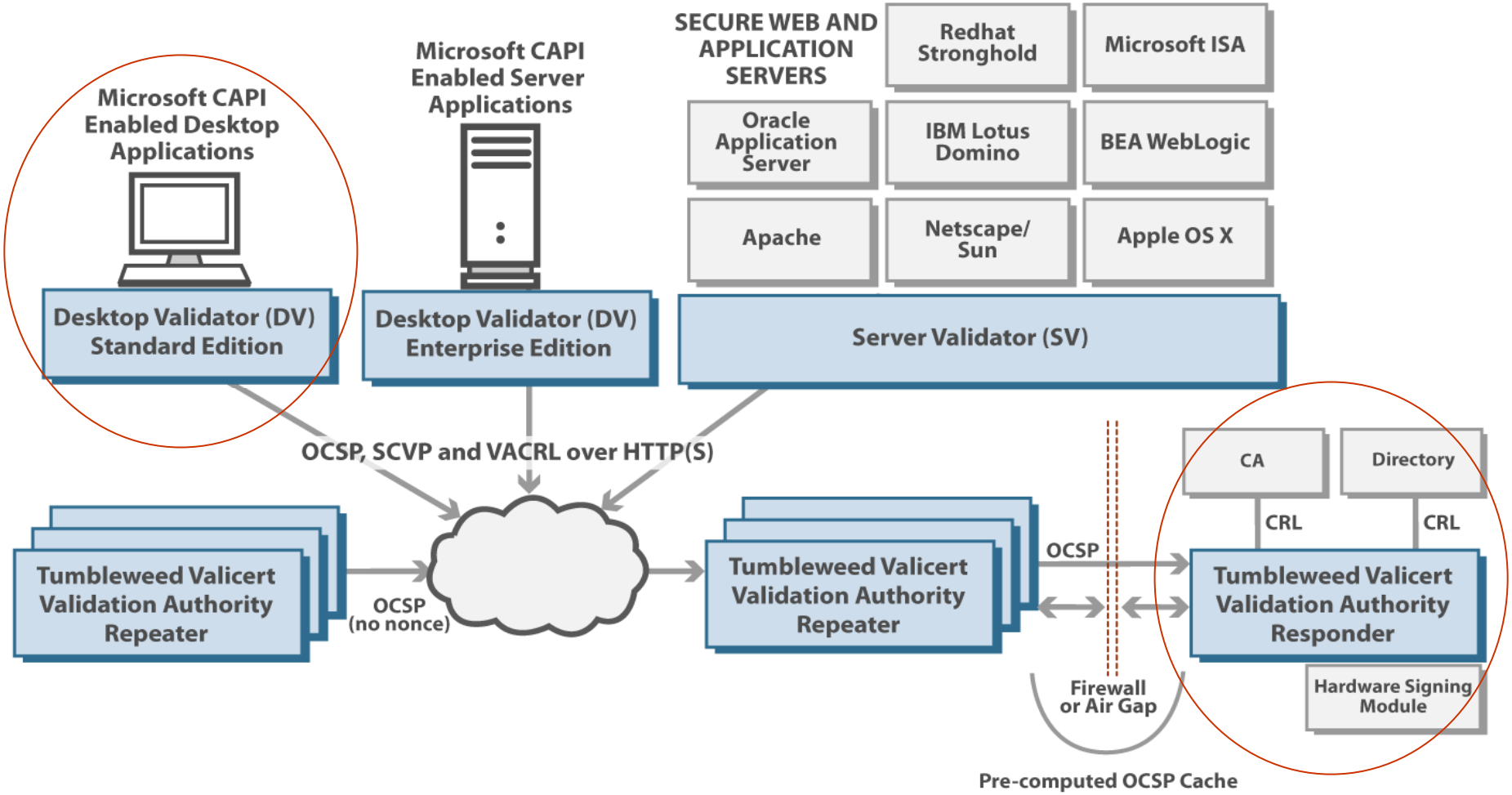
Tumbleweed®

- Desktop Validator (DV) is a lightweight PKI client for Windows
  - **PDVAL TWG Qualified Vendor's List**
- Designed to perform delegated path validation (DPV) in the Outlook email application.
- By enabling the DV Outlook Add-In, DV will enhance Outlook's default local path validation operation and perform a delegated path validation operation utilizing SCVP to communicate to a trusted VA Server.
- The trusted VA Server will return the validated discovered certificate path to DV which will add it to the local CAPI store.
- DV can be configured to optionally perform path validation

Client/Server/Distributed architecture

Tumbleweed®

Today's typical OCSP based certificate validation architecture



PDVAL Challenges

Tumbleweed®

- **How to force Windows applications to use discovered paths**
  - Updating CAPI store may not be enough.
  - CAPI only allows one root install at a time
  - Move to OCSP vs SCVP full discovery
- **Some Windows applications require restart.**
  - LSAS is a good example
- **Windows CryptoAPI has its own path building procedure**
- **One PDVAL path test resulted in 1,000+ paths being created**
- **The tests brought out a couple of tests where Windows actually failed when the expected result was good.**

PDVAL Challenges

Tumbleweed®

- **Path Building in MS CAPI and Web Servers**
  - MS CAPI and Web Servers currently do not allow path building to be delegated to trust providers or web server APIs
  - Adding trusted root requires user intervention
  - Default path discovery must succeed before validation plugins are executed
  - Default process differs among different Windows system (NT, 2000, XP, 2003)
  - No certificate policy processing in Windows 2000

PDVAL Checklist

Tumbleweed®

- **Survey applications**
- **Determine Trust Anchors**
- **Consider application based vs. delegated PDVAL**
- **Review qualified vendors**
  - http://www.cio.gov/fbca/validation_solutions.htm
- **Consider outsourced vs. in-house managed services**

Tumbleweed®

Questions & Answers

- **Contact Information**

Ann Smith
Vice President, Federal Sales
Phone # 703-248-6931
Email address: ann.smith@tumbleweed.com

Steve Ebbets
Sr. Systems Engineer
Phone # 703-918-4863
Email address: steve.ebbets@tumbleweed.com