Public Key Infrastructure

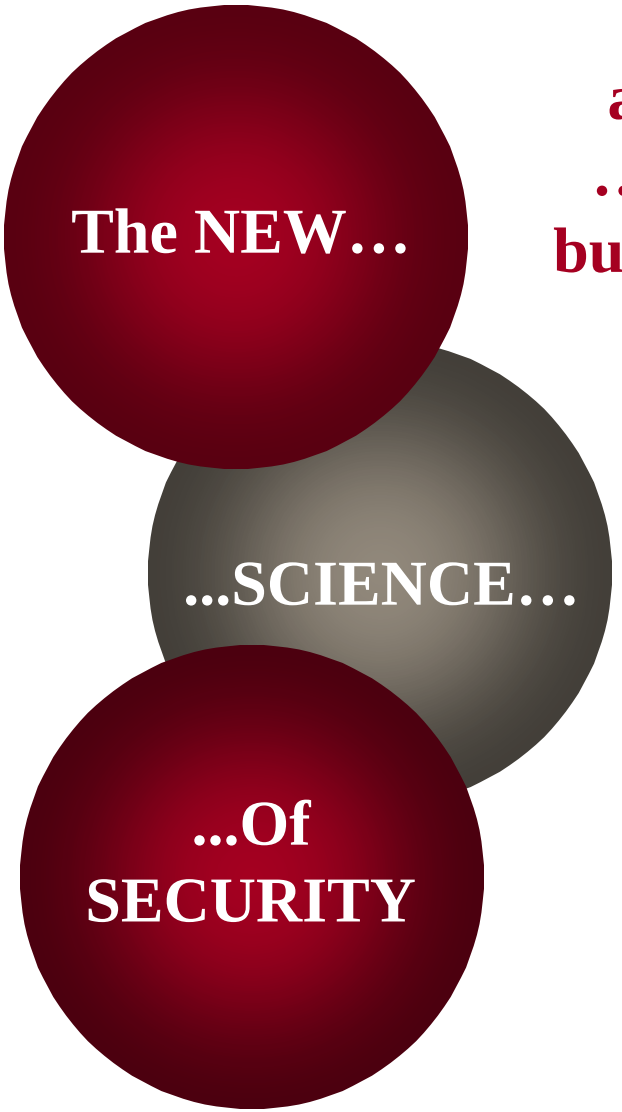
Ed Bassett

June 21, 2001

ENSPHERICS

... provides custom designed security solutions for a variety of clients who operate in high risk, high threat and high profile environments through responsive, specialized teams of talented technologists.

Enspherics



as in "new economy" …security for the way business gets done today.

as in "applied science"…practical solutions that will protect your information right now.

as in "it's all we do"…pure and total focus on this complex, mission-critical area.

ENSPHERICS

Outline

- Introduction
- Quick technology overview
  - Digital signatures
  - Digital certificates
  - PKI
- Why PKI?
  - Typical scenarios
- Got PKI?
  - Why it’s easier than you think!

ENSPHERICS

Business Drivers

- Market Forces
  - Legacy EDI technology focuses on static business relationships
  - E-commerce technology focuses on dynamic business transactions
    - Informal or no prior arrangements between parties
    - Digital signatures enable this type of transaction
    - Integrity often more important than privacy

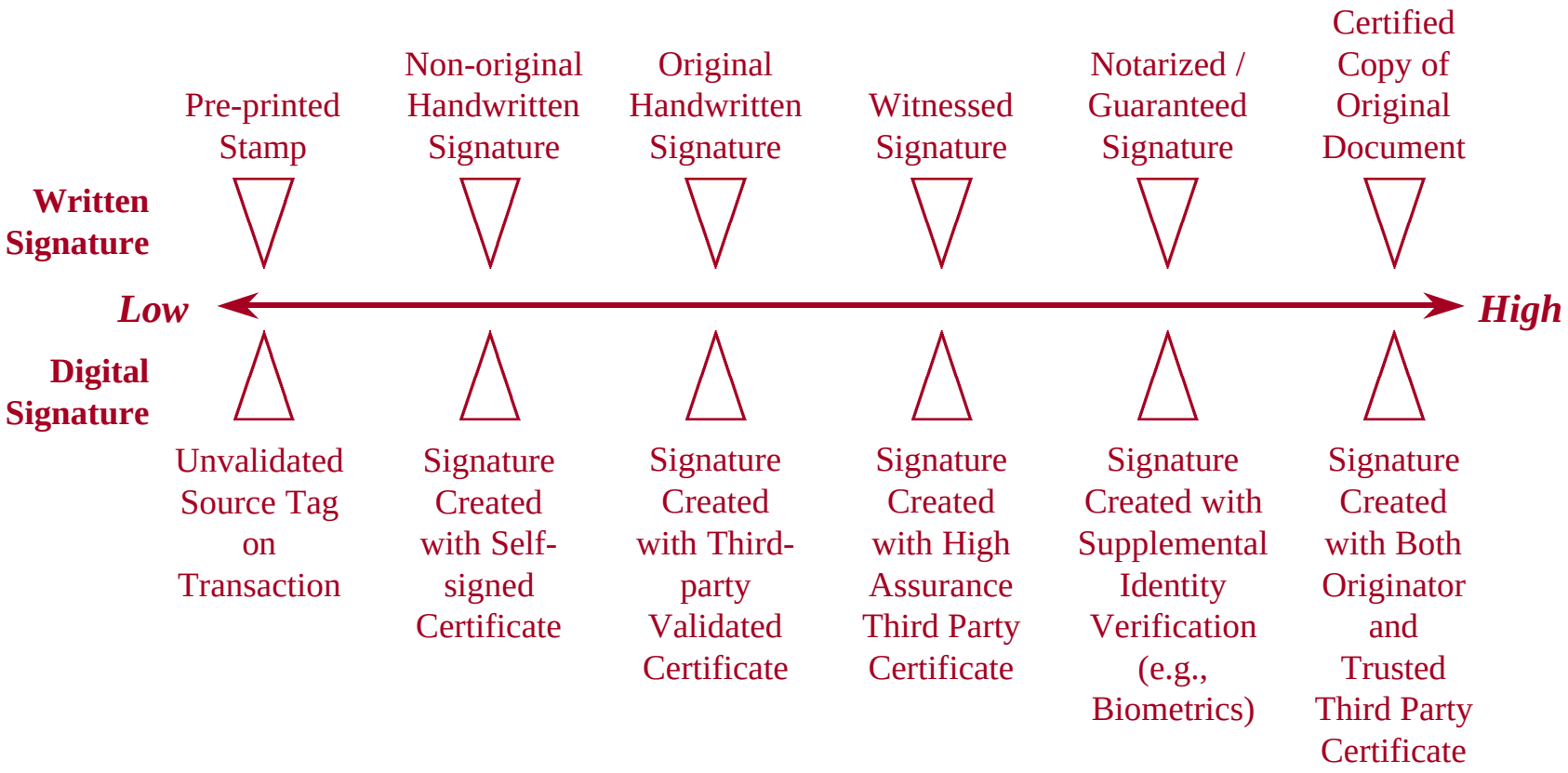
ENSPHERICS

Business Drivers (Cont.)

- Electronic transactions need assurance features analogous to paper transactions
  - Validation of content
  - Identity of sender
  - Non-repudiation
- Need forgery protection similar to paper documents
- “Original” is an irrelevant concept
- Public key encryption is the base technology

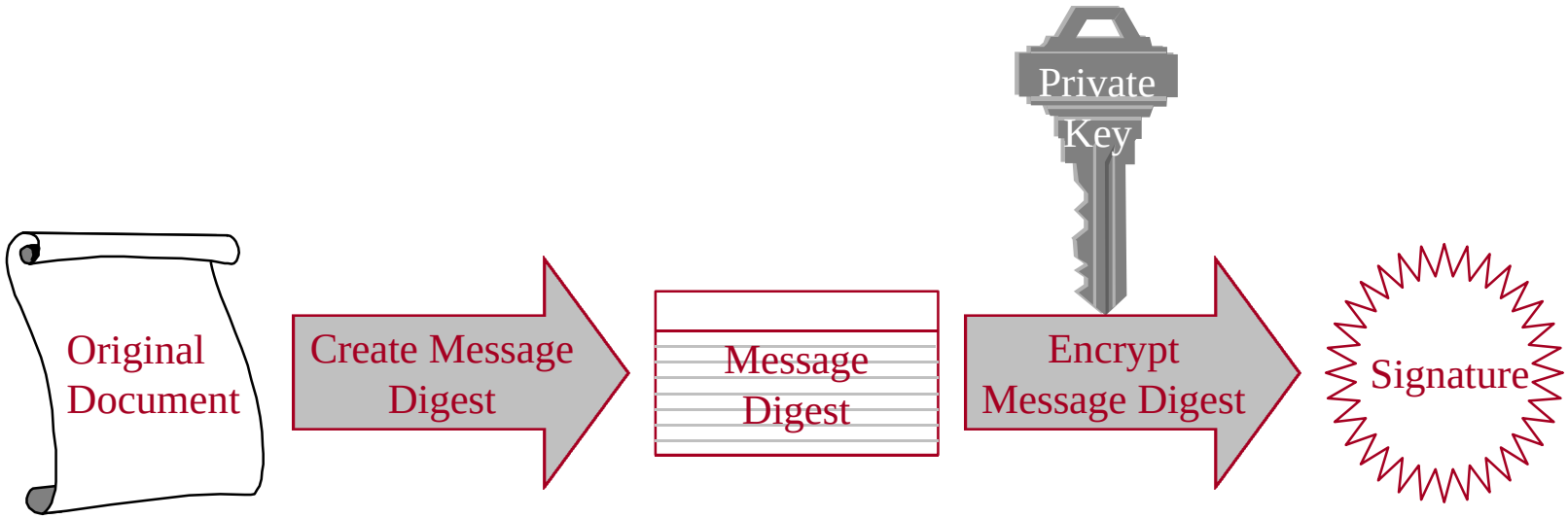
ENSPHERICS

Assurance Spectrum



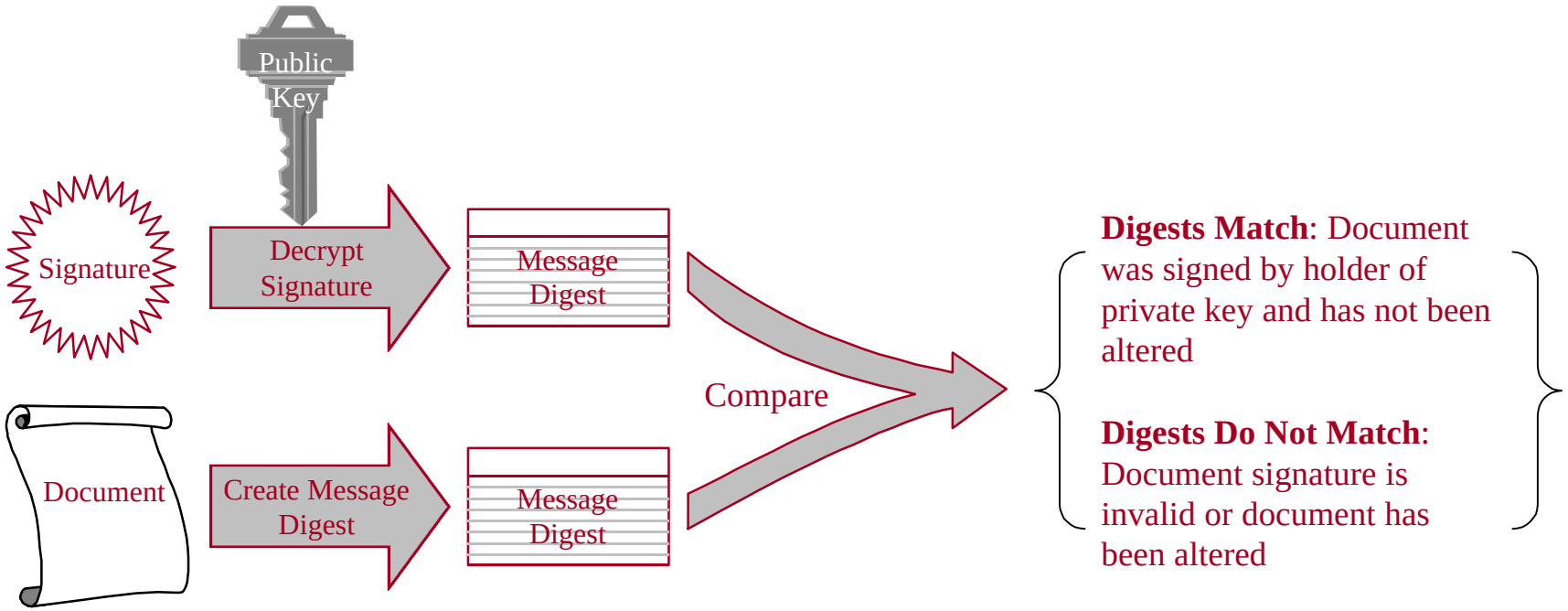
ENSPHERICS

Creating a Digital Signature



ENSPHERICS

Checking a Digital Signature



ENSPHERICS

Digital Certificates

- Digital certificates add assurance
  - Trusted third party binds identity (e.g., Person's name) to a key pair
  - Provides recipients with confidence of signature authenticity
  - Various levels of assurance of "binding"

ENSPHERICS

PKI Overview

- Public Key Infrastructure (PKI) is the set of supporting services that enable public key based security to be used on a wide scale
  - Certificate management technology
  - Interoperability standards
  - Legal support for digital signatures

ENSPHERICS

PKI Overview (Cont.)

- Digital signatures provide
  - Authentication of identity -- who sent the transaction
  - Integrity of contents -- what was sent
  - Non-repudiation -- cannot later deny sending transaction
- PKI provides
  - Means of managing digital signature keys
  - Third party “certification” of the binding between identity and keys

ENSPHERICS

Why PKI?
Typical Scenarios

- Occasional or one-time customer transactions
- Recurring customer transactions
- Internal workflow
- Business partner interaction

ENSPHERICS

Occasional Transactions

- Scenario
  - Health care provider needs to verify source and content of records requests submitted by patients
- How PKI is used
  - Patients obtain certificates from public certificate issuers ahead of time
  - Patients present certificates to provider at the time a request is placed
  - Provider verifies the certificate to ensure it is signed by a trusted third party and that it has not been revoked
  - Patients fill out a request form and sign it using their private key
  - Provider verifies the signature using the certificate

ENSPHERICS

Occasional Transactions (Cont.)

- Business Considerations
  - Similar to customer signature on paper request form
    - Digital signature used primarily to ascertain identity in case of dispute
  - Provider may accept certificates issued by a number of different issuers
    - Each must use identity verification procedures sufficient to benefit the provider in case of a dispute over the signature
  - No need for a prior exchange of credentials between the provider and patient

ENSPHERICS

Recurring Transactions

- Scenario
  - Insurance company has an established relationship with a health care provider
  - Insurer needs to protect transactions such as claims, payments, web delivery status information
- How PKI is used
  - Insurer issues a “private label” certificate to provider
  - Certificates used by providers only for transactions with the insurer
  - Providers present certificate and use private key to sign documents submitted to the insurer

ENSPHERICS

Recurring Transactions (Cont.)

- Business considerations
  - Digital signature assures insurer that provider is actually authorizing the claim/request
  - Provider cannot later deny having made the transaction or dispute its contents, since signature is attached
  - Assurance supported by existing business relationship between parties

ENSPHERICS

Internal Workflow

- Scenario
  - Hospital needs to ensure electronic forms have proper authorization/approval signatures
- How PKI is used
  - Hospital issues internal certificates to authorized employees
  - Employees use private keys to create digital signatures on forms they approve
  - If/when needed, hospital can verify signature using the employee's certificate

ENSPHERICS

Internal Workflow (Cont.)

- Business Considerations
  - Digital signature created with and stored with completed form
    - Personal accountability for actions
    - Easy auditable
  - Analogous to employee identification badges used for facility security purposes
  - May not need certificates when binding between people and key pairs is determined by the business itself (as opposed to a trusted third party)
    - Other key management methods could be used

ENSPHERICS

Business Partner Interaction

- Scenario
  - Health care network members need to exchange business documents using a public (un-secure) network
- How PKI is used
  - Partners exchange digital certificates ahead of time
  - Sender uses private key to create digital signature on document
  - Sender uses recipient's public key to encrypt document
  - Recipient uses private key to decrypt document
  - Recipient uses certificate of sender to verify signature

ENSPHERICS

Business Partner Interaction (Cont.)

- Business Considerations
  - Signing sensitive documents protects against tampering and provides a lasting record of origin
  - Encryption of data ensures privacy when transmitting sensitive information over public communications media (e.g., Internet)
  - Self-signed certificates might be used in place trusted third party certificates
    - Must be verified out of band (e.g., compare certificates verbally)

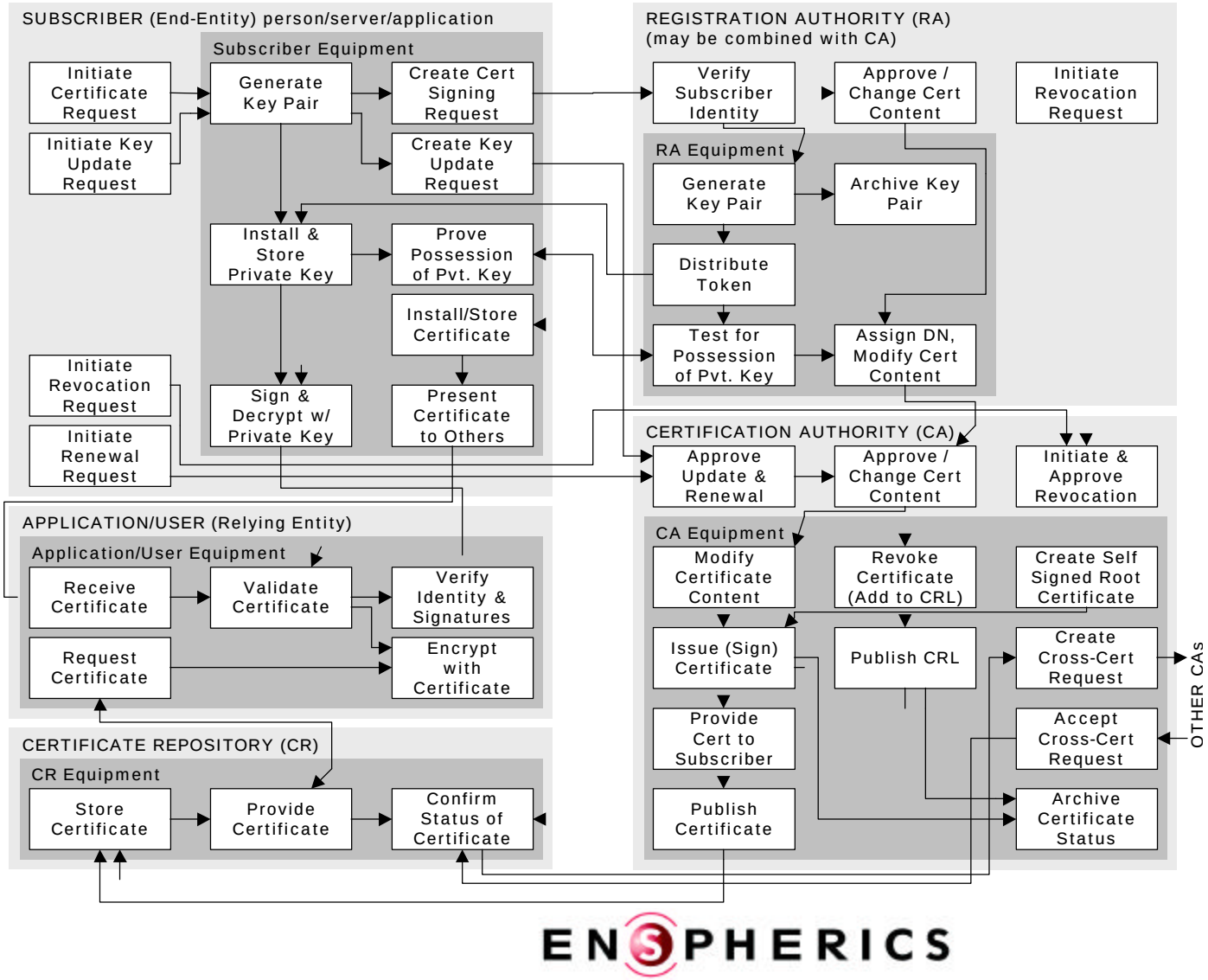
ENSPHERICS

Got PKI?

- PKI has high perceived barriers to entry
  - Technology is esoteric
  - Image is larger than life
    - Underlying technology used for many different business needs
  - Hype has preceded reality
  - Scope, schedule, and cost of PKI projects is not clear

ENSPHERICS

Looks Hard?



ENSPHERICS

PKI Components

- Core PKI functions
  - Registration authority (RA)
  - Certification authority (CA)
  - Certificate repository (CR)
- End Entities
  - Subscribers
  - Relying parties

ENSPHERICS

Options to Implement PKI

- Vendor offerings oriented toward three distinct models for implementing a PKI
  - Outsource the PKI to a trusted third party
  - Build the PKI with components
  - Buy a PKI that is complete out-of-the-box

ENSPHERICS

Example Solution 1: Outsourced PKI

- Overview
  - This solution would involve the use of third party to provide CA services
- Primary components of this example solution
  - CA equipment: PKI Vendor
  - RA equipment: PKI Vendor (typically web interface)
  - CR equipment: PKI Vendor Directory
  - Subscriber equipment: Unmodified web browsers and servers (Netscape, Microsoft)
  - Application/User equipment: Unmodified web browsers and Servers (Netscape, Microsoft)

ENSPHERICS

Outsourced PKI

Description of Basic Operations

- The CA, RA, and CR equipment located at the Vendor facility
- “Local Registration Authority” (LRA) is used to delegate RA functions to customer locations

ENSPHERICS

Outsourced PKI

Significant Features and Advantages

- Rapid deployment
  - Vendor supplies all necessary software and user interfaces
  - Vendor will also supply policy documents (or models that can be easily modified), training, procedures, and implementation advice.
- Proven software tools and policies/procedures
- Less need for specialized expertise
- High availability
- Secure key generation
- High-security of the CA keys

ENSPHERICS

Outsourced PKI

Significant Features and Advantages (Cont.)

- Scalability
- Advancement of features
- Compliance with standards
- Cost for small deployment
- Increased user acceptance/trust of CA

ENSPHERICS

Outsourced PKI

Significant Limitations and Disadvantages

- Certificate functions rely on long-haul communications
- Cost for large deployment
- Limited ability to modify
- New features delivered at vendor option/pace
- Complex liability issues

ENSPHERICS

Example Solution 2: Build with Components

- Overview
  - This solution would involve the use of PKI components integrated to perform all PKI functions
- Primary components of this example solution
  - CA equipment: PKI vendor
  - RA equipment: PKI vendor
  - CR equipment: Directory vendor (typically LDAP)
  - Subscriber equipment: Unmodified web browsers and server
  - Application/User equipment: Unmodified web browsers and servers

ENSPHERICS

Build with Components

Description of Basic Operations

- Single tool provides the CA and RA functions
- Subscriber-side PKI functions provided by built-in functions in client and server software already deployed

ENSPHERICS

Build with Components

Significant Features and Advantages

- Rapid deployment
- Cost effective for incremental deployment
- Standards compliant
- Easy acceptance and learning curve for subscribers

ENSPHERICS

Build with Components

Significant Limitations and Disadvantages

- Lack of certificate life cycle management features
- Limited extensibility to non-web applications

ENSPHERICS

Example Solution 3: Buy Out of the Box

- Overview
  - Use one comprehensive vendor solution for all PKI functions
- Primary components of this example solution
  - RA/CA/CR equipment: PKI vendor
  - Subscriber equipment: Client browser plug-in from PKI vendor
  - Application/User equipment: Proxy, web server plug-in, or application shim/plug-in from PKI vendor

ENSPHERICS

Buy Out of the Box

Description of Basic Operations

- Vendor has already integrated the PKI components
  - Deployment consists of installing the components and configuring the interface tools to match local policy
  - The plug-in modules perform authentication, authorization, and encryption/decryption functions on web browser—server communications

ENSPHERICS

Buy Out of the Box

Significant Features and Advantages

- Robust certificate management tools
- Tight integration between PKI components
- Interoperability with other applications using the PKI vendor's API

ENSPHERICS

Buy Out of the Box

Significant Limitations and Disadvantages

- User interface learning curve
- Support for new browsers/servers
- Proprietary methods
- Client modifications

ENSPHERICS

Conclusion

- Business drivers are clear
- Plentiful, mature vendor offerings lower barriers to entry
- Options for insertion of this technology make PKI a realizable capability

ENSPHERICS

Conclusion

- Current/future trends in PKI life cycle
  - Low/no footprint clients
  - Web form signing
  - Additional assurance features e.g., timestamp
  - Enhanced registration options (in person; automated/self serve)
  - Token storage of certificates for two-factor authentication
  - Common policy frameworks
  - Common methods for certificate management

ENSPHERICS

Contact Information

Ed Bassett

Enspherics, Inc.

5675 DTC Blvd

Englewood, CO 80111

(303) 850-0495

ebassett@enspherics.com

www.enspherics.com

ENSPHERICS