PKI
Past Present & Future

Ashutosh Saxena

Outline

- Motivation
- PKC and PKI
- PKI examples
- PKI criticisms & obstacles
- PKI evolution
- The road ahead…

Motivation

- We have crossed 15 yrs of formal PKI service in INDIA. (Remember IT Act 2000)
- Has our understanding and usgae of this technology grown in any way?
- With evolution of both theory & technology, where we are heading towards!!

PKC and PKI

- Public key cryptography
  - Each entity in a collection has a pair of keys
    - Alice has pub_A, $priv_A$
    - Enc, d-sig. possible (mathematical operations)
    - RSA, ECC, Bilinear Pairing, Lattice based, etc...

- Public Key Infrastructure (PKI)
  - Makes PK cryptography available to applications and environments that wish to use it
    - Enc, d-sig. possible (security operations)
  - Key pair bound to an entity identifier in a way that makes it useful to a variety of apps

PKI (cont'd)

- "Identifier"
  - Uniquely, without ambuguity, specifies entity within some context or environment, but may not necessary reveal actual identity
  - Context/environment need not be global in scope (depends on apps that will use keys)

PKI (cont'd)

- Binding of key pair and identifier
  - Validity of bindings
    - Authority (making & breaking)
    - Issuance process (syntax & dissemination)
    - Termination process (alerting)
  - Use of bindings
    - Key management process ("One/All purpose")
    - Binding validation process (trusting someone else's key)

Outline

- Motivation
- PKC and PKI
- PKI examples
- PKI criticisms & obstacles
- PKI evolution
- The road ahead…

PKI Examples

- Over the past years, there have been several approaches to model and implement PKI
- Like X.509, PGP, SPKI, etc.

Sample Comparisons

PKI Solution	Authority	Issuance Process
X.509	CA, AA. CA is owner / definer of namespace.	ASN.1 syntax. X.500 or LDAP directories.
PGP	No external authority. User is owner / definer of namespace.	Issued by key owner (e.g., Web page, e-mail sig., key server).
SPKI	Authorization granter. Relying party is owner / definer of namespace.	Issue authorizations based on pseudo Ids.

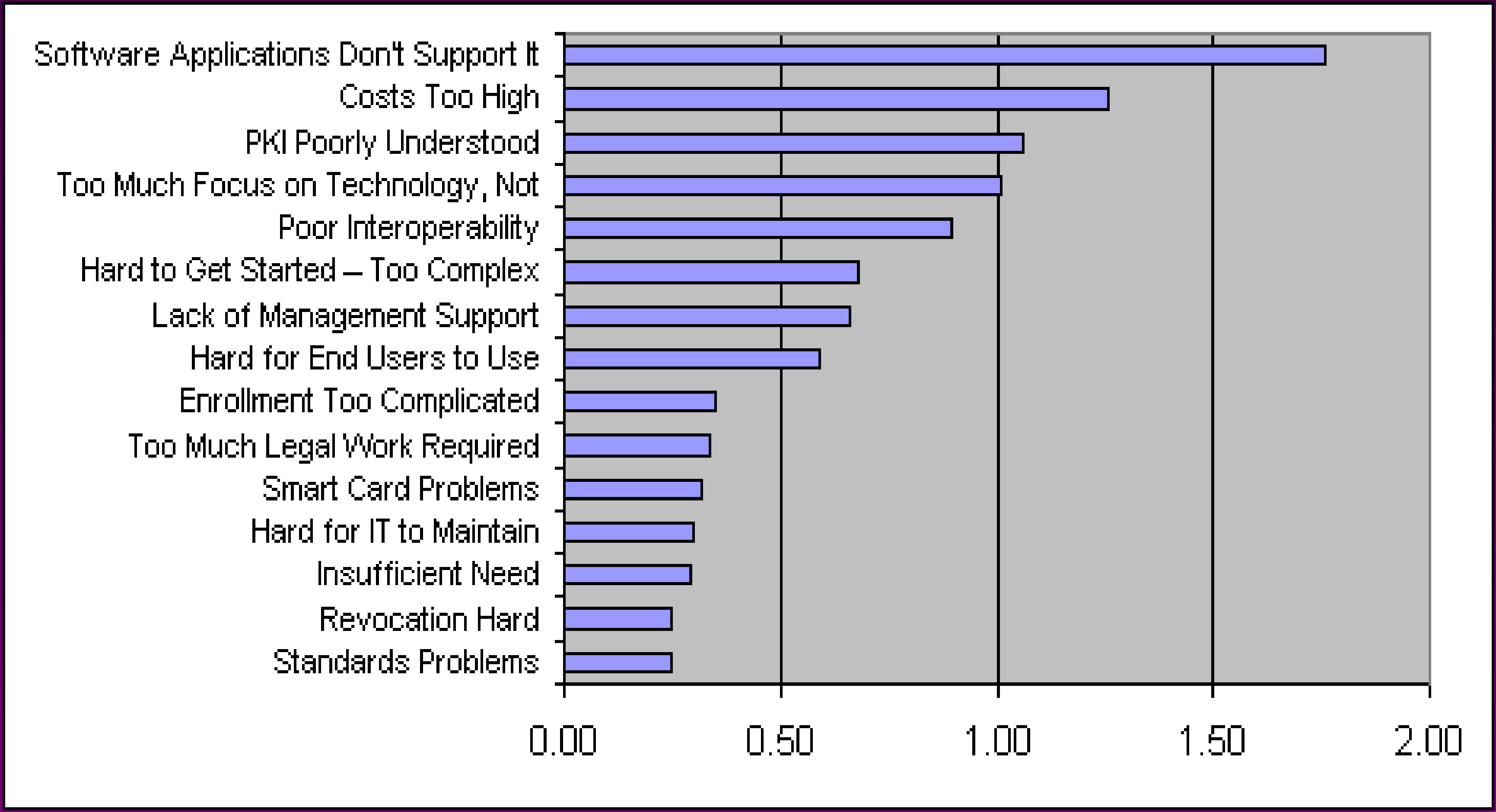
Outline

- Motivation
- PKC and PKI
- PKI examples
- PKI criticisms & obstacles
- PKI evolution
- The road ahead…

PKI Criticisms & Obstacles

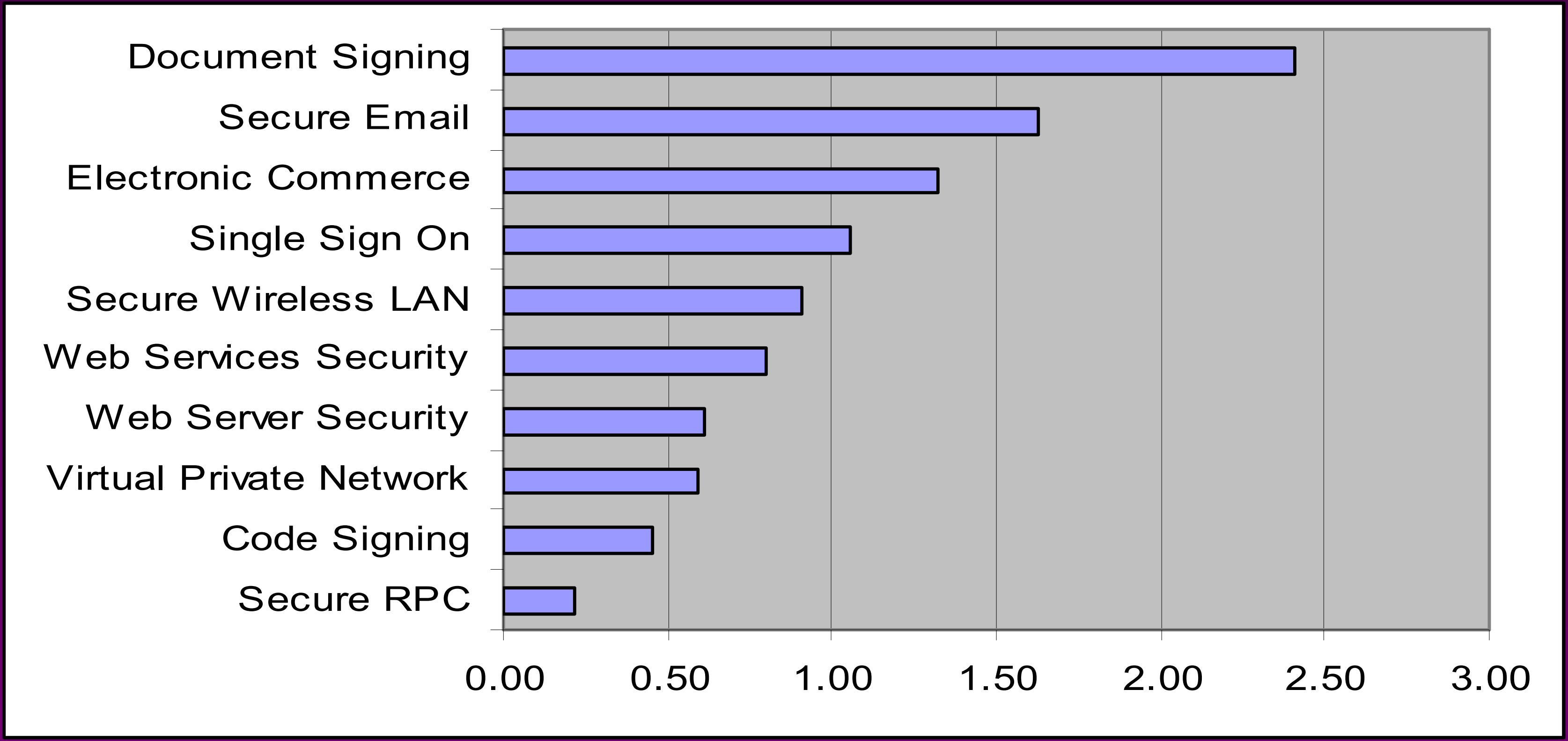
- Many criticisms have been leveled at this technology
- Probably the best-known collection is the “10 Risks” paper by Ellison & Schneier
- But criticisms cannot always be taken at face value: need to consider whether the “flaw” being criticized is actually related to PKI or not

Obstacles: Ranked by Importance

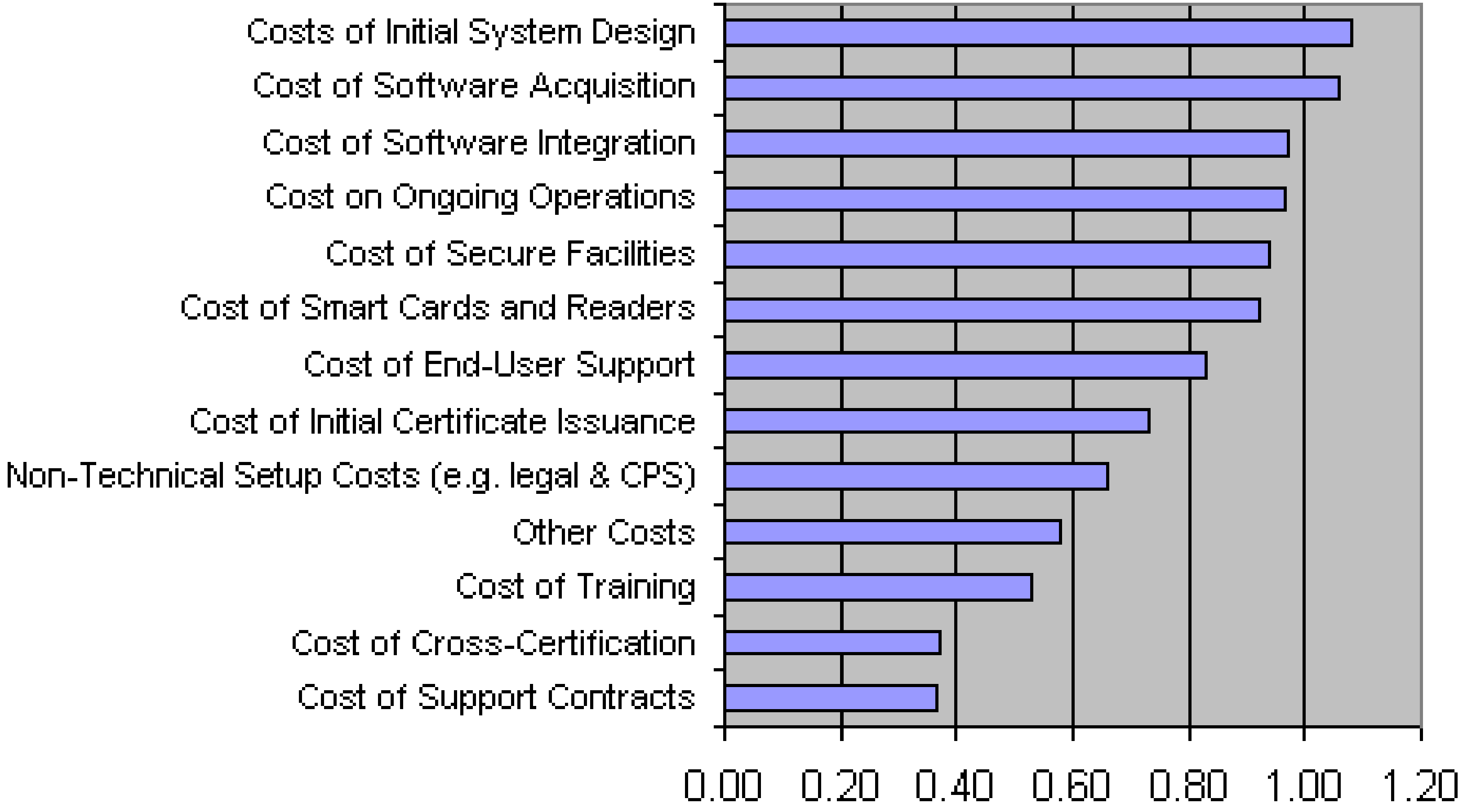


The first four obstacles have more than half of the total points

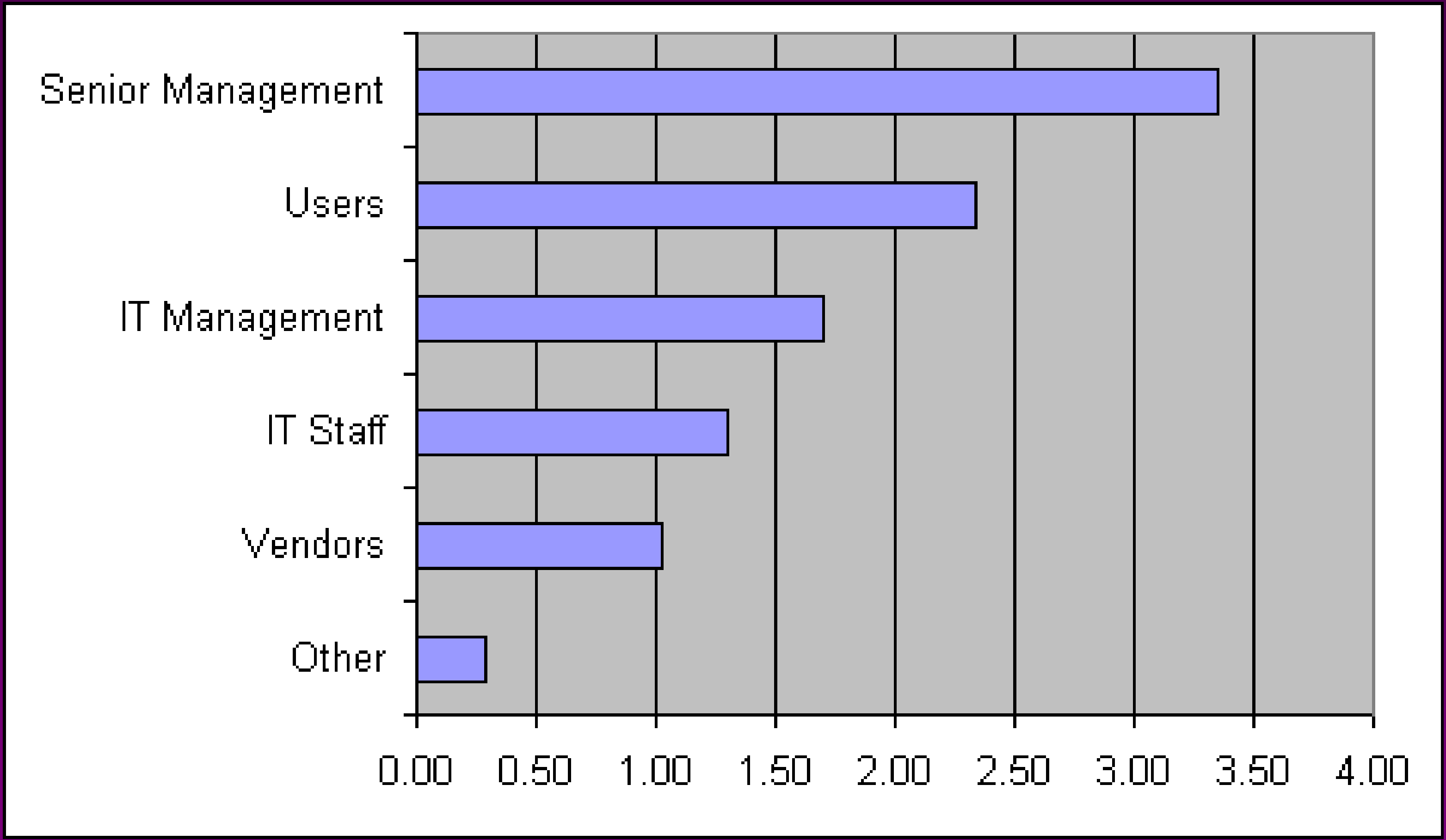
Applications: Ranked by Need for Improvements in PKI Support



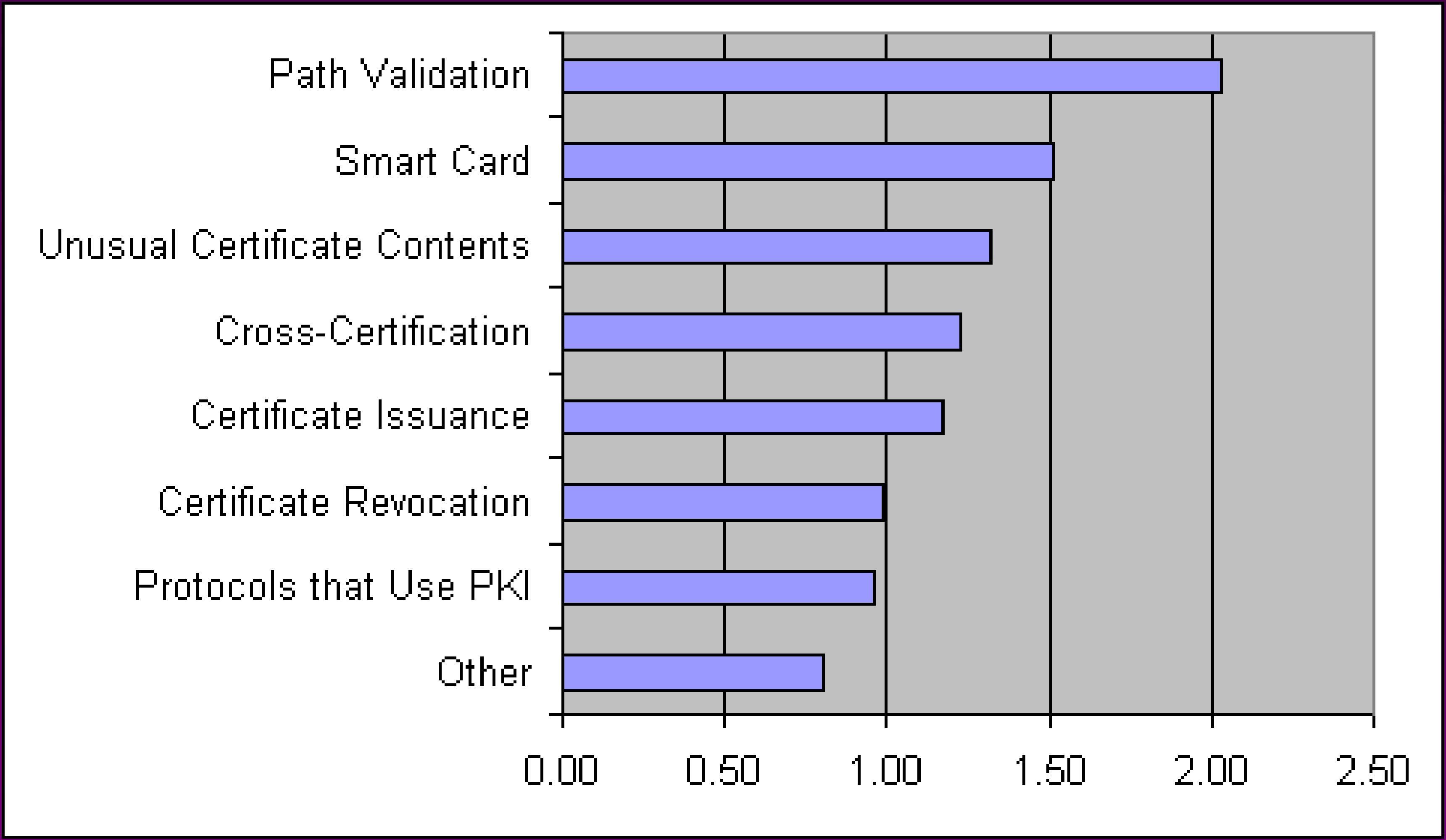
Costs Ranked



Parties: Ranked by Greatest Need for PKI Understanding



Where the Most Serious Interoperability Problems Arise



Outline

- Motivation
- PKC and PKI
- PKI examples
- PKI criticisms & obstacles
- PKI evolution
- The road ahead…

Evolution

- In the year 1993 version of the ISO/IEC CCITT/ITU-T IS X.509 began to be disseminated, recognized, and implemented in small-scale environments
- Late 1993 / early 1994 was effectively the birth of PKI (although the acronym was yet to be coined)
  - Infrastructural considerations were paramount (how to make PK technology available to a wide variety of applications)

Evolution (cont'd)

- Initial definition (1994)
  - Authority: always and only a CA
  - Issuance: X.509 syntax; DN; X.500 Directory
  - Termination: CRL; X.500 Directory
  - Anchor: root of CA hierarchy
  - Private key: CA gen.; local storage
  - Validation: large, special-purpose s/w toolkit

Evolution (cont'd)

- After more than a decade of extensive discussion, research, and implementation by numerous interested parties world-wide:
  - Each of the 6 components has broadened quite considerably with deeper understanding
  - BUT, the same 6 components comprise the core of the definition (i.e., the essential characteristics of the definition remain unchanged)

Evolution (cont'd)

- Current definition
  - Authority: multiple choices (incl. RAs)
  - Issuance: multiple choices (syntax)
  - Termination: multiple choices (incl. online)
  - Anchor: multiple choices (augment & diminish)
  - Private key: multiple choices (gen., reg., storage)
  - Validation: mult. choices (thin client; native apps)

Outline

- Motivation
- PKC and PKI
- PKI examples
- PKI criticisms & obstacles
- PKI evolution
- The road ahead…

Future of PKI

- Moving from theory to practice
  - Over ten years, innovative thinking, fruitful technical discussion, constructive criticism, and implementation efforts have driven the recognition of the need for options
  - Research into secure architectures and secure protocols have made options possible
  - BUT options have yet to be embraced in a significant way in real products

Future of PKI (cont’d)

- ✔A priority area to be addressed is better certificate processing in complex cases.
- ✔Multiple sources of revocation status (CRL, OCSP, indirect CRL, . . .) require careful definition of procedures when building the certificate path up to a trusted root and verifying the status of all certificates in chain.
- ✔An exact API needs to be defined and implemented as a library to support Applications.
- ✔This would make PKIs more suited to real-world needs

Conclusion

- The goal of this discussion is to convey that the PKI community has significantly broadened its understanding of this technology.

- The challenge now is to translate that understanding to real PKI deployments that solve authentication challenges in real, heterogeneous environments.