

An Examination of Asserted PKI Issues and Proposed Alternatives

John Linn (RSA Laboratories), Marc
Branchaud (RSA Security)

3rd PKI R&D Workshop

NIST

April 2004

DRAFT, 4 April 2004

Presentation Structure

- Introduction
- Asserted Issues
- Proposed Approaches
- Conclusions

Motivations

- Many issues have been raised about PKI over time
- Many variations have been proposed
- Which issues are valid?
- Do the alternatives resolve the issues?
- How would useful results appear in context?

Why PKI isn't pervasive: three possible causes

- PKI technology is suitable, but awaits motivating demand for secure applications
 - Important hypothesis to consider, but not this paper's focus
- PKI technologies are hard to deploy, or deliver limited or less-needed value
- PKI is perceived to imply and require higher assurance than is necessary in many environments

Some Elements Assumed in Contemporary PKI Baseline

- Support for hierarchic and non-hierarchic trust models
- Revocation via CRLs or basic on-line queries like OCSP
- Support for various name forms
- NB: Once upon a time, each of these were novel...

Issue: Difficult to Retrieve Keys and Certificates

- It can be hard to obtain a PKI certificate
 - If no directory exists for publication
 - If that directory isn't accessible or can't be located
 - If the certificate is needed by an off-line user
- Interest in avoiding or simplifying public-key processing preconditions

Issue: Value of Certified Keys

- The trusted key is the goal, and certificates are a mechanism
- Certificates were developed to represent keys in a protected fashion on an untrusted repository
- If keys are obtained over a secure channel from an on-line trusted server, value of certification diminishes

Issue: Certificate Processing Complexity

- It's complex to process certificates, and to integrate their processing with applications
 - Interpreting key usage indicators, ...
- Validation and path-level processing add further complexity
- Have certificates grown to include an unwieldy amount of free-standing data?

Issue: Costly Certificates

- Common assumption: certificates are expensive, so can only be issued rarely and sparingly
- High-assurance enrollment procedures are appropriate in some contexts, but not always needed
- Certificates/assertions can be issued dynamically

Issue: Problematic Cross-Domain Trust Management

- Enabling trust between unrelated entities is a daunting challenge, administratively and technically
- Conventional PKI reflects trust between domains, not between principals
- Policy mapping provides mechanism, but may not fit practices
- Manual trust anchor management is a common and limiting constraint

Issue: Naming Semantics

- PKIs bind keys to names, but not all names have the same properties
 - PKI names can be local vs. global
 - PKI names can match or diverge from names used in other contexts
 - PKI names can imply paths or can be independent of them
- What properties are most useful?

Issue: Use with Insecure Clients

- PKI designs have anticipated deployments where users securely control keys
- Many common platforms are subject to compromise
- Can provide useful security even in “commercial practice” environment
 - Various methods can improve assurance
 - Even without perfect client protection, PKI-based services can still be useful

Issue: Privacy Compromises

- Conventional PKI certificates provide signed linkages between principals and actions
- Persistent keys become identifiers
- Certified identities can be used for profiling
 - Validation servers can be well-placed observers...

Issues to Proposals

- Several categories of issues have been asserted
- Several types of proposals have been made, responding to different concerns
- Goal: consider value and implications

Proposal: IBE and Related Methods

- Several variants on Identity-Based Encryption have been defined
- Many allow a sender to prepare a message for a recipient without obtaining the recipient's certificate
- Sender needs parameters for recipient's domain, implying need for cross-domain infrastructure
- Basic IBE approach implies intrinsic key escrow

Proposal: PKI with On-Line TTP

- On-line TTPs can achieve IBE-like properties
 - Encrypting with a TTP's public key
 - Encrypting with a recipient's key, which the TTP can provide (or generate)
- Dynamic certificate generation can also serve other purposes (temporary attributes, login sessions)

Proposal: Distributed Computation Methods

- When platform compromise or constrained trust is an issue, can limit impact
 - By storing principal keys on a protected server, requesting remote operations
 - By distributing key elements and performing cooperative computation
- Provide assurance at overall system level, rather than per-component

Proposal: Alternative Validation Strategies

- CRLs operate off-line, but provide coarse revocation latency
- On-line services can provide finer latency, but require trust and availability
- Hash trees optimize CRL-like properties, with particular value at large scale

Proposal: Key Servers

- If on-line servers are fully trusted for path-level discovery and validation of certificates, it's an incremental step for them to provide keys directly
- Clearly simplifies clients, but also changes assurance model and assumptions

Proposal: Privacy Protection Approaches

- Can certify (temporary) pseudonyms
- Can separate attributes into individual certificates, presented selectively
- Can aggregate or anonymize status queries
- Alternate certification models provide qualitatively stronger protection, but could require new operational paradigms

Observations

- PKIs have addressed broad and difficult problems with partial success
 - Technologies can reflect organizational conflicts, can't generally resolve them
- Self-contained certificates allow off-line processing, but with management and complexity costs
 - Useful to decouple assumptions about certificate properties

Conclusions

- PKIs, in suitable forms, remain essential substrates for secure transactions
 - Need various means to securely provide keys for different contexts
- Methods and their assurance levels should reflect requirements, need not lead them
 - Conventional vs. dynamic vs. no certificates...
 - Appropriate tradeoffs among client protection, client processing, server trust