



X. 509 V3 Revisited Past, Present, and Future

Warwick Ford
VeriSign, Inc.
wford@verisign.com



Outline

- **Past**
 - Original X.509
 - Internet Privacy Enhanced Mail
 - X.509 Version 3
- **Present**
 - Deployment
 - Issues
 - Retrospect
 - Alternatives
- **Future**

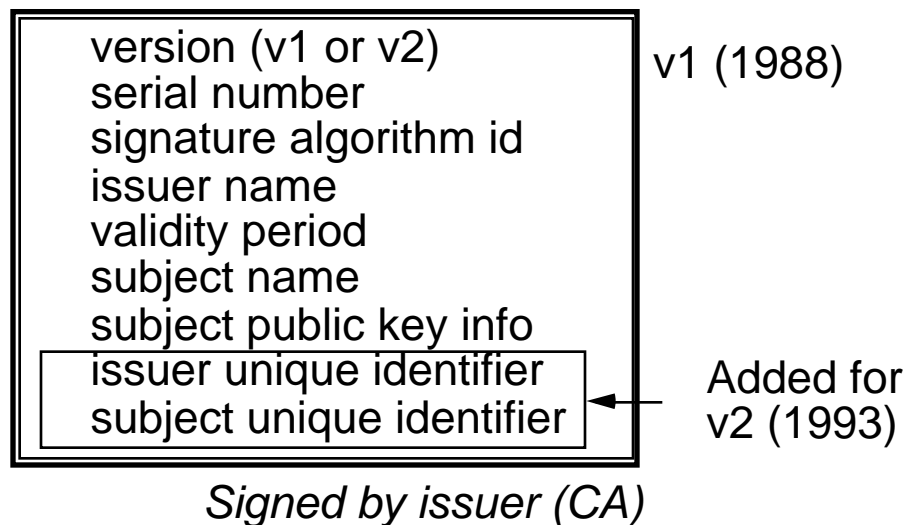
The Basic Problem

- I want to reliably know the public key of party X with whom I wish to communicate securely
- A certificate, digitally-signed by a certification authority, binds a public key to the identity of its owner
- I already reliably know the public key(s) of one or more certification authorities —root CA(s)
- A certification path exists from a root CA to party X

X.509 - Past

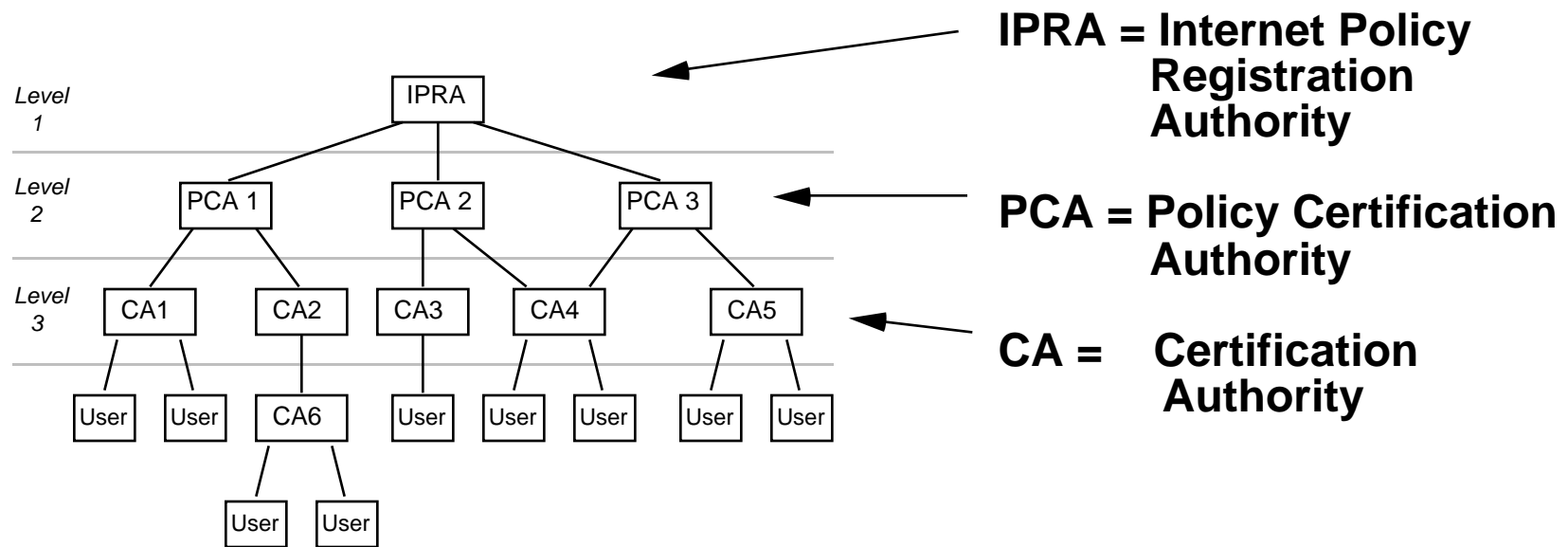
- **Original X.509**
 - 1988
- **Privacy Enhanced Mail**
 - 1993
- **Version 3 Extension Mechanism**
 - 1995
- **Standard Extensions**
 - 1996

Original X.509



- **First published
1988 - v1 certificate**
- **Extended 1993 for
directory access
control - v2
certificate**

Internet Privacy Enhanced Mail



- **RFC 1422 - 1993**

Problems - Naming and Directories

- An X.500 name does not necessarily map easily to application names, e.g., e-mail name for PEM
- An X.500 name does not adequately identify a subject to a certificate user
- X.500 directories are not ubiquitous
- Even if there is an X.500 directory, cannot necessarily get meaningful identification information securely

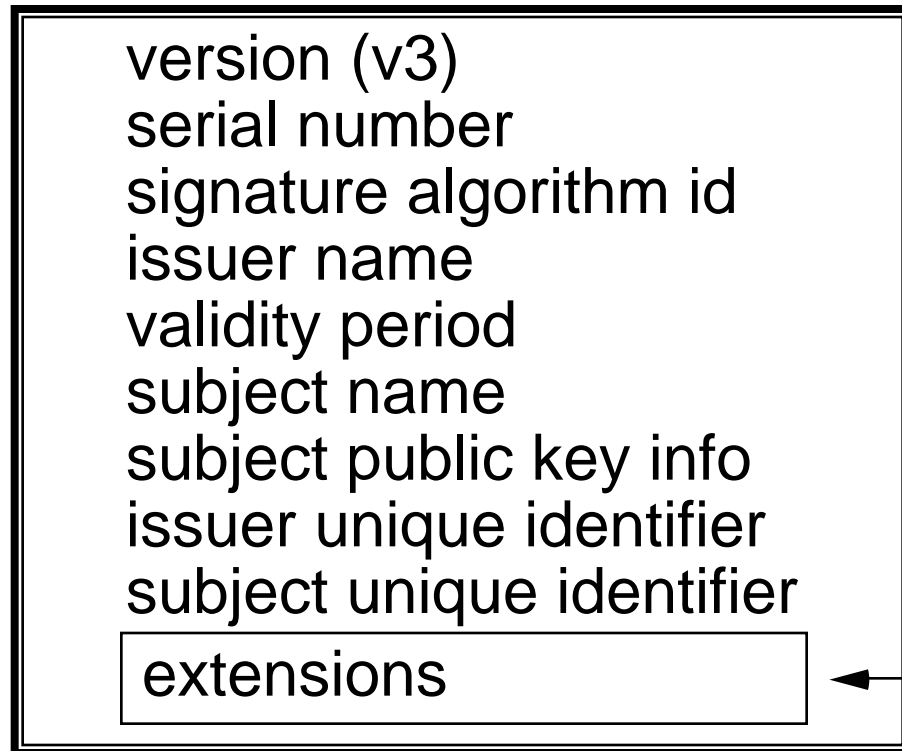
Problems - Trust Relationships

- The PEM hierarchy is too rigid for everyone
- Certificate chains should start at the point of most trust — not necessarily the top of a hierarchy
- PCAs are an unwieldy way of managing policies
- Name subordination rule does not fit with natural X.500 naming structures

Other Problems

- No support for key life cycle
- No identifiers for different keys
- No support for key usage purpose
- Nowhere to convey authorization information
- Certificate revocation lists can grow unbounded

Version 3 Certificate



Signed by issuer (CA)

criticality
flag

extn.a	cf	value
extn.b	cf	value
extn.c	cf	value

Version 3 Extensions

- Specific extensions can be defined in standards or by user communities
- Standard certificate extensions:
 - subject attributes, alternative name forms
 - policy identifiers
 - constraints
 - key identifiers, etc.
- Standard certificate revocation list extensions:
 - partitioning, revocation reasons

X.509 - Present

- **Deployment**
 - Who is using X.509?
- **Issues**
 - ASN.1
 - Names
 - Authorization
 - Other
- **Version 3 in retrospect**
- **Alternatives**
 - SDSI, SPKI, “Short Certificates”

Deployment

- **SSL**
 - Server authentication, encryption
 - Client authentication
- **S/MIME**
 - The 1997 wave ...
- **SET**
 - Visa, Mastercard, ...
- **DoD Defense Messaging System**

Implementing Vendors

- Microsoft
- Netscape
- virtually everyone

Issues - ASN.1

- Nobody likes it
- The specs are difficult to find, understand
- It makes life very easy for the specifier
- It makes life hard for the low-budget implementor
- After initial investment, it ceases to be a concern to implementors
- There is no good alternative

Issues - Names

- **X.509 V3 brought almost unbounded flexibility to names (e.g., e-mail address, account number, anonymous reference)**
- **Do you need a name at all?**
- **How important is the global X.500 hierarchy?**
- **Are name constraints important? ...too complex?**

Issues -Authorization

- Is X.509 for authentication only?
- Can you put authorization information in X.509 v3 extensions?
- Do we need standardized authorization certificates?
- Are ANSI X9 attribute certificates the answer?

Issues - Other

- Trust models - does the X.509 v3 trust model serve the purpose?
- Proprietary extensions - why have a standard if you do not achieve interoperability?

Retrospect - What v3 Did Well

- The “open” approach to standard establishment - combined efforts of ISO/IEC, ITU, ANSI X9, IETF, government (most debating done on an open IETF list)
- The extension mechanism
- The attention to Internet requirements
- The flexible naming

Areas for Reflection

- **Complexity - especially the chain validation algorithm**
- **ASN.1 as the sole representation syntax**
- **Authorization not addressed**
- **The policy mechanism is yet unproven**

Alternatives

- **SDSI (Rivest and Lampson)**
 - Nice syntax
 - Simple naming structure
 - Support for groups
- **SPKI (IETF)**
 - Nice syntax
 - Authorization is the primary goal
- **“Short Certificates”**
 - Under study in ANSI X9

X.509 vs. Alternatives

- Nothing is new - most of the SDSI and SPKI debates have been had before
- X.509 v1 was genuinely “simple” - experience proved it *too* simple
- X.509 v3 design was heavily requirements driven (including legal perspective)
- Features such as policies and constraints are needed and are *not* simple
- X.509 v3 is a good fit for open commercial PKI
- SDSI and SPKI are good fits for certain environments (especially access control)

X.509 - Future

- **Work continuing on:**
 - profiles
 - policies and practices
 - supporting PKI protocols
 - cross-certification
- **Better specifications, tools emerging**
- **Link to authorization certificates (ANSI? SPKI?)**
- **Industry commitment to interoperation**