X.509

(1985-1988)

Some reminiscences for X.509 Day May 9th 2022

By Doug Steedman
CCITT Special Rapporteur on Directory Systems, 1985-1988

Disclaimer

This presentation is a trip down memory lane for me, covering a period more than 35 years ago. I haven’t even thought about these events very much in the interim, even when wrangling X.509 certificates as a software engineer (something I do to this day).

Thus, I am not speaking in any way on behalf of my employer (Google).

Also, I’m not 29 any more (my age when I started the work under discussion) and my memory ain’t what it used to be, so please forgive any anachronisms or other lapses.

X.509: why me ?

- From 1981-1984 I was active in the MHS (Message Handling Systems) CCITT Special Rapporteur group, led by Ian Cunningham of Bell-Northern Research (BNR), Ottawa, Canada.
    - I worked for BNR (and Ian) at the time
- In 1984, after the MHS group produced the X.400 series, it was decided to spin off “Directory Systems” as a separate group for the following study period (1985-1988).

X.509: why me ?

- For 1985-1988
  - Jim White led the continued work on MHS (X.400)
  - I got the new Directory Systems role
- Jim and I had worked very closely together on MHS
  - we jointly designed X.409 “Presentation Transfer Syntax and Notation” (which became ASN.1)
  - Our close collaboration continued and we attended and actively contributed to each others’ teams work

X.509 standard: design philosophy

- Standards committees were sometimes thought of as political forums where ugly compromises were reached without technical coherency
- In contrast, the MHS group tried to operate like an international design team
- Directory Systems (including X.509) followed this same philosophy
- Participating organizations brought in their own contributions, but the group endeavored to fit their ideas into an overall clean design
- There was little or no “cramming in” of incompatible ideas so both contributors could claim victory
- This made it satisfying to work on, and may explain why people worked so hard (we were often only barely aware of whatever beautiful city we were in).
- The people who attended my meetings were, pretty much without exception, smart, hard-working, creative (also multi-lingual). I am very happy to have worked with them and appreciative of their efforts.

Why did the Directory Systems group create X.509?

- We were mandated among other things to work on authentication both for our own use and for MHS
- The Directory had an interesting role as both a user and provider/facilitator of authentication
- We were (I think) the first standard to employ Public Key Cryptosystems.
    - We of course used RSA in particular (as an examplar). (I have the letter from RSA Inc. authorizing its use in a standard).
- The use of public-key cryptography and certificates seemed to fit in well with our concept (conceit?) of the Directory as a global-scale massively distributed database
- Directory components and user agents use certificates and signatures to securely communicate
- Other applications can do similarly, using the Directory to access any certificates necessary

Why was the standard called X.509 ?

(Actually CCITT had “Recommendations” not “Standards”).

- We had decided how the work should be split up into different Recommendations
- They were still called X.ds*n* (for various small integers *n)*. Directory Systems: Authentication Framework was X.ds8.
- At some point in late 1987, we got a phone call from CCITT in Geneva (don’t remember who took or made the call). We had been allocated the X.500 series ! (That was great news, we had thought there was a possibility we would be allocated some subrange of X.400).
- We allocated the numbers within our range by analogy with X.400. X.500 introduced all the concepts, much like X.400 did for Message Handling.
- We viewed the Authentication Framework a general technique usable outside of Directory Systems, just as ASN.1 was usable outside of MHS. So we called it X.509 by analogy with X.409.

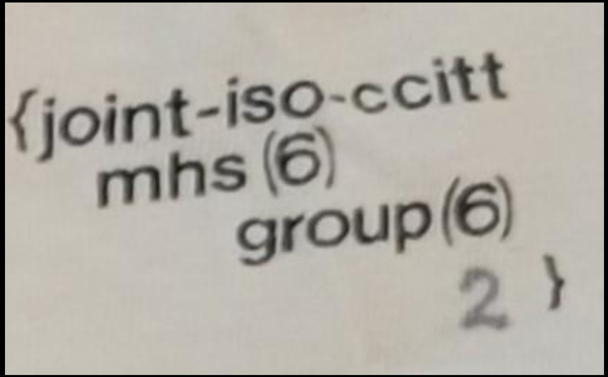
X.500: notable meeting locations

Despite what I said about hard work, some meeting locations were amazing, and the hosts did drag us off for bus trips and banquets time to time

- Fall 1984, Directory System unofficial pre-meeting MELBOURNE. (Coach trip for wine tasting, zoo, and beautiful scenery)
- Sept 1985, FIRENZE. Ad hoc meeting in “Orangerie” @ Villa Le Rondini
- March 1987. MÜNCHEN over Fasching. Wow!
- November 1987. GLOUCESTER, England, hosted by British Telecom in grand style. We took over a hotel/conference center for 3 weeks)
- GENEVA (frequently). Wish I was there now!
- ISO meetings (e.g. EGHAM – near Windsor Castle).

ISO Collaboration

- The X.500 standards were among the first to be produced collaboratively between CCITT (then ITU-T) and ISO
- It was interesting to be in on the action when that collaboration was coming together. The organizations had hitherto been rivals with very different modes of working
- On X.500 series, we ended up working so closely that I (the CCITT Special Rapporteur) ended up chairing an ISO editing meeting
- My wonderful collaborator from the ISO side was Hoyt Kesterson II. Hoyt is “here” today.
- A tangible symbol of that was the ASN.1 Object Identifier tree (heavily used in X.509), which had three top level nodes: iso, ccitt, and joint-iso-ccitt.
- X.509 had been a potential area of disagreement: strictly speaking the ISO directory group had no mandate to work on authentication; a different group was tasked to define security standards



{joint-iso-ccitt
mhs (6)
group (6)
2 }

Doug: since X.500 days

- Continued to work on standards during 1989-1992 (Open Distributed Processing, ASN.1, ROS)
- Worked as a consultant and taught classes on ASN.1 and X.500
- Wrote books on each of those topics
- In 1991, went back to my first love: programming
- I moved to California and joined General Magic (to work for Jim White!). Worked on “Telescript” and Mobile Agents.
- In 1996 joined WebTV just after their acquisition by Microsoft
- Worked for Microsoft doing security software for Set-Top Boxes (WebTV, MSTV, Mediaroom) until 2013
- Joined Google where I work on security software for Google’s consumer devices (e.g. Chromecast, Google Home, Google Wifi, and Nest products)