your name, (seth hardy)
your shoe size, (12)
your identity? (?)

what do we trust in this web?

defcon 14 – 06 aug 2006

i. introduction

who am i?

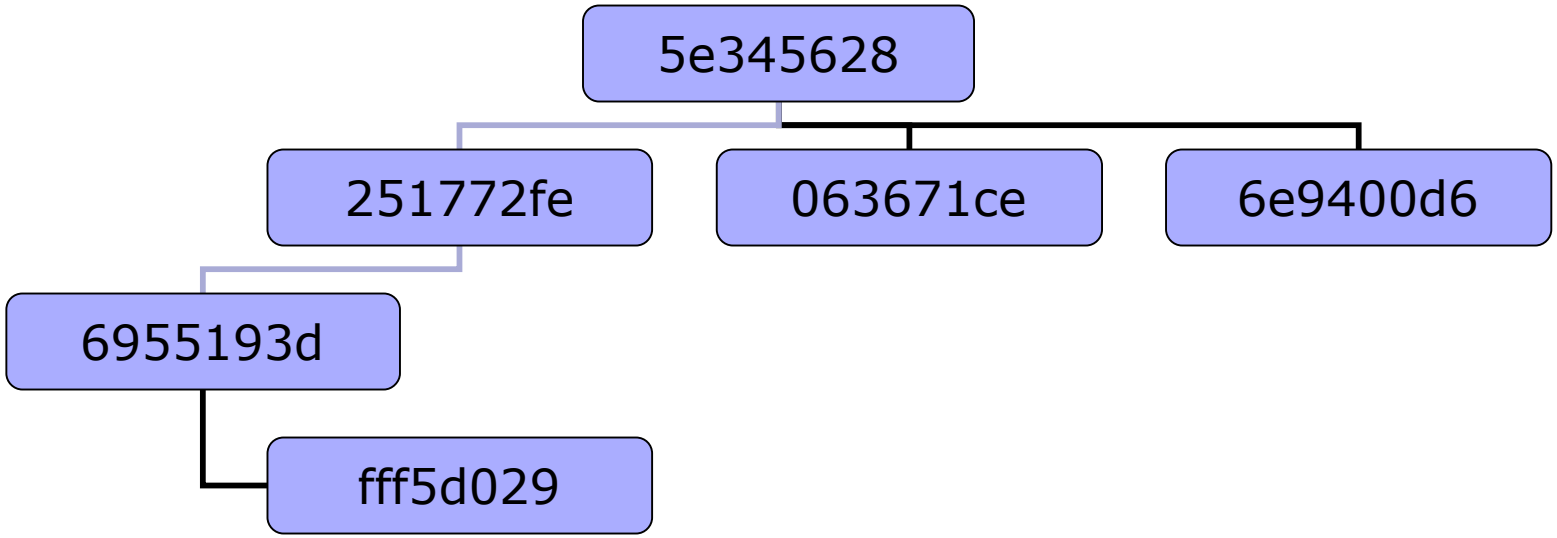
- what do you mean?
  - the name on my birth certificate is “seth hardy”
  - online i often use the handle “shardy”
- maybe you don’t care who i am, just that i’ve done this before
  - defcon
  - black hat
  - ...etc.

why give this talk?

- it all started 2 years ago
- first, the 5hope keysigning party
- then, the defcon 12 keysigning “party”
  - (there was booze but not so much keysigning)
- later that year, there were issues with keysigning at 21c3 (and it was much worse at 22c3)

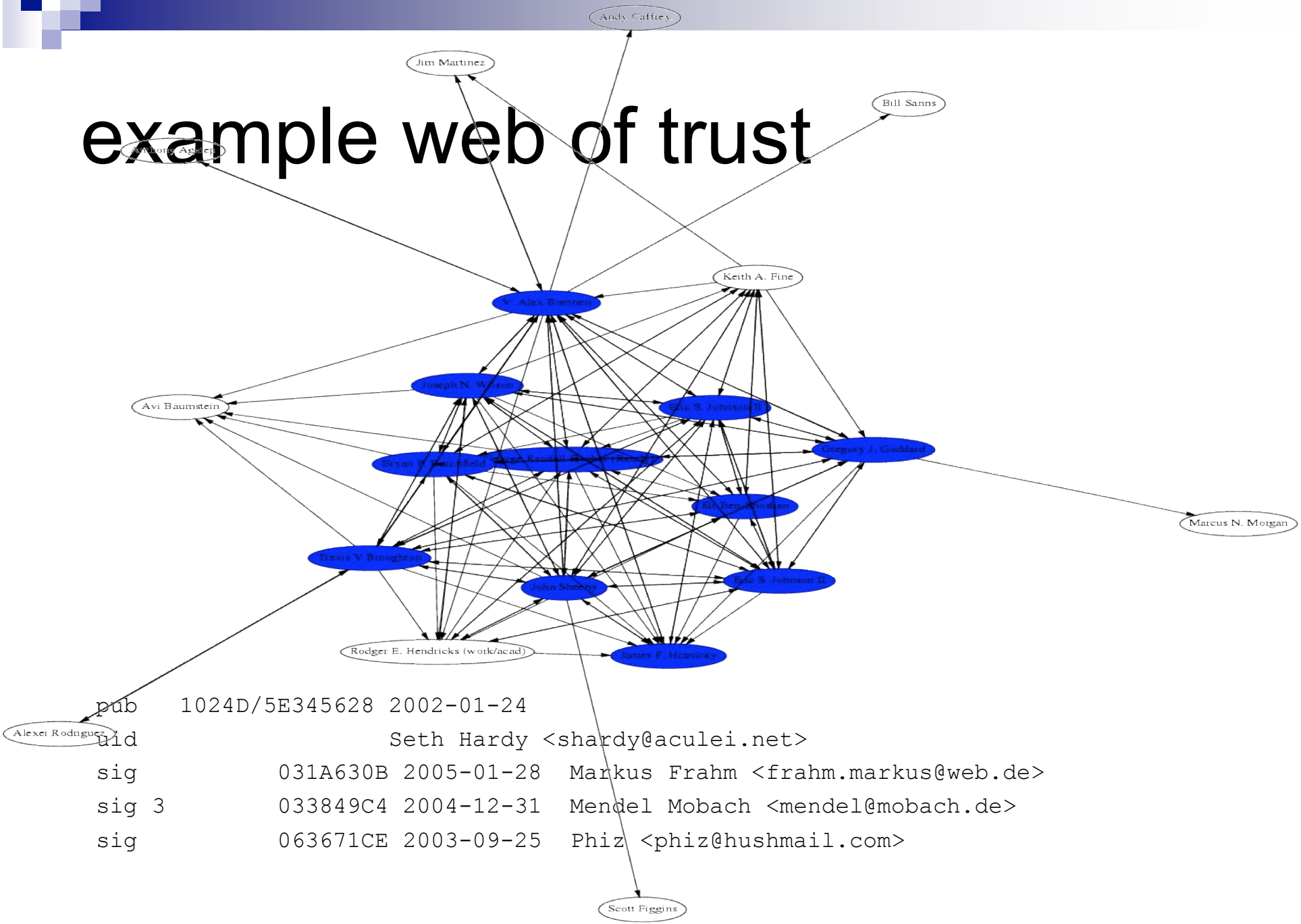
ii. background

why a web of trust?



trust the validity of keys you've never seen before!

example web of trust




```
pub   1024D/5E345628 2002-01-24
uid                  Seth Hardy <shardy@aculei.net>
sig          031A630B 2005-01-28  Markus Frahm <frahm.markus@web.de>
sig 3        033849C4 2004-12-31  Mendel Mobach <mendel@mobach.de>
sig          063671CE 2003-09-25  Phiz <phiz@hushmail.com>
```

iii. signing practices

standard keysigning practices

- verify that a key is accurate
  - check the fingerprint
- verify that key ownership is accurate
  - check the name against photo id
  - send key to email address

but, what about...

- what do we do about pseudonyms/handles?
- what do we do about organization keys?
- who is security-officer@netbsd.org?
  - they have 24 signatures
  - they have signed 3 other keys
  - only three hops from my key

```
$ gpg --fingerprint f8376205
pub   1024R/F8376205 1997-07-01
      Key fingerprint = 19 57 B6 26 AB F1 81 A4  A4 F9 4E CE F5 27 4C F5
uid                  security-officer@netbsd.org
```

signing policies

- exactly what it sounds like: people coming up with strict policies for what they will and won't sign
- writing and publishing a signing policy is definitely a Good Thing...
- ...because it lets everyone know whether you have a good policy or a bad one
- there are all sorts of interesting policies...

common signing policies

don’t make me call your parents:

The signee must prove his/her identity to me by way of a valid identity card, passport or driving license. These documents must feature a photographic picture of the signee. No other kind of documents will be accepted. Please note that I require that proof of identity even for people I know personally. This verification step is called "proof of identity".

common signing policies

i keep mine tattooed on my ass, thank you very much:

I will then ask the signee how the secret key is protected. I appreciate people publishing their key policy on the world wide web like I do, but I accept an explanation how the key is protected as well. Please note that I will publish the protection scheme in my key signing notes.

common signing policies

isn’t there a reason we can sign uids individually?:

If one of the UIDs fails the test a warning will be sent to one of the other mail addresses and the procedure will be halted until a satisfactory explanation has been received or the procedure has been cancelled by the signee. Keys with only partly verified UIDs will be deleted and cannot be signed. Please note that this only applies to email addresses - ICQ-IDs will not be signed, photos will be signed if I can recognize the person on the photo to be the signee.

common signing policies

nobody challenges photo ID:

The signee must prove his/her identity to me by way of a valid identity card, passport or driving license. These documents must feature a photographic picture of the signee. No other kind of documents will be accepted. Please note that I require that proof of identity even for people I know personally. This verification step is called "proof of identity".

will you take this one?

(my id doesn't look like this, it's a few years old)

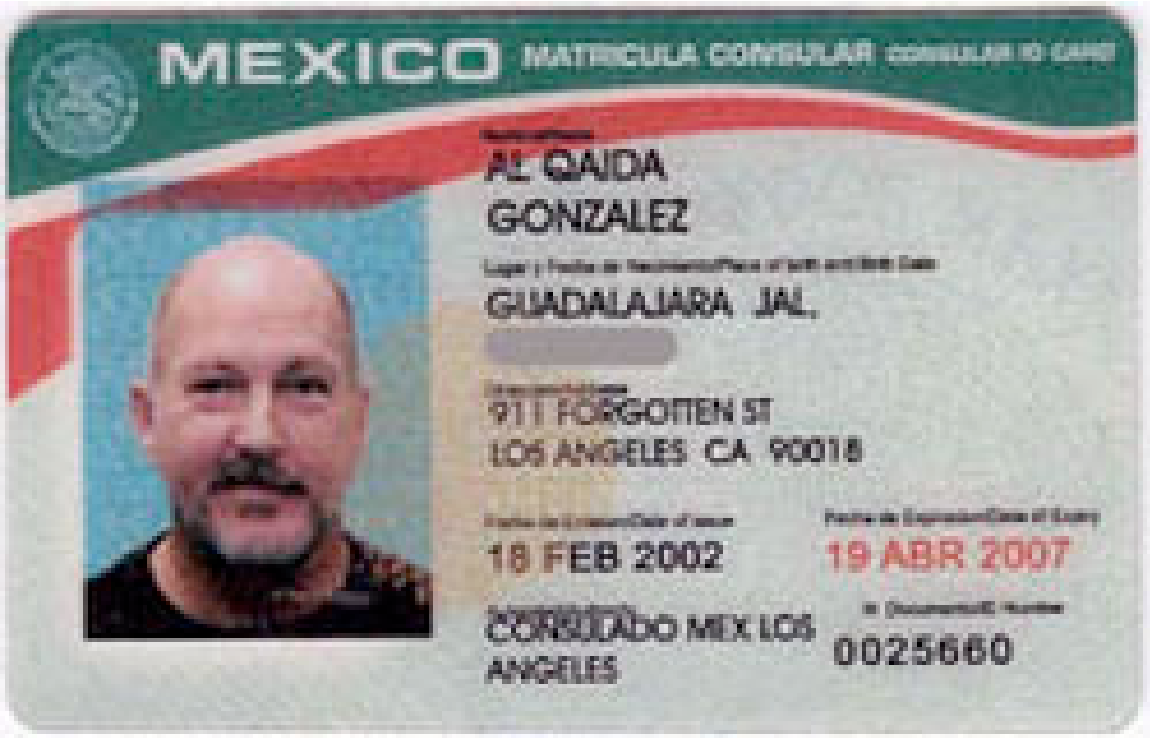
how about this one?

(canadians are people, too. also, thanks to jeremy for placing the contents of his wallet online for anyone to grab.)

or this one?

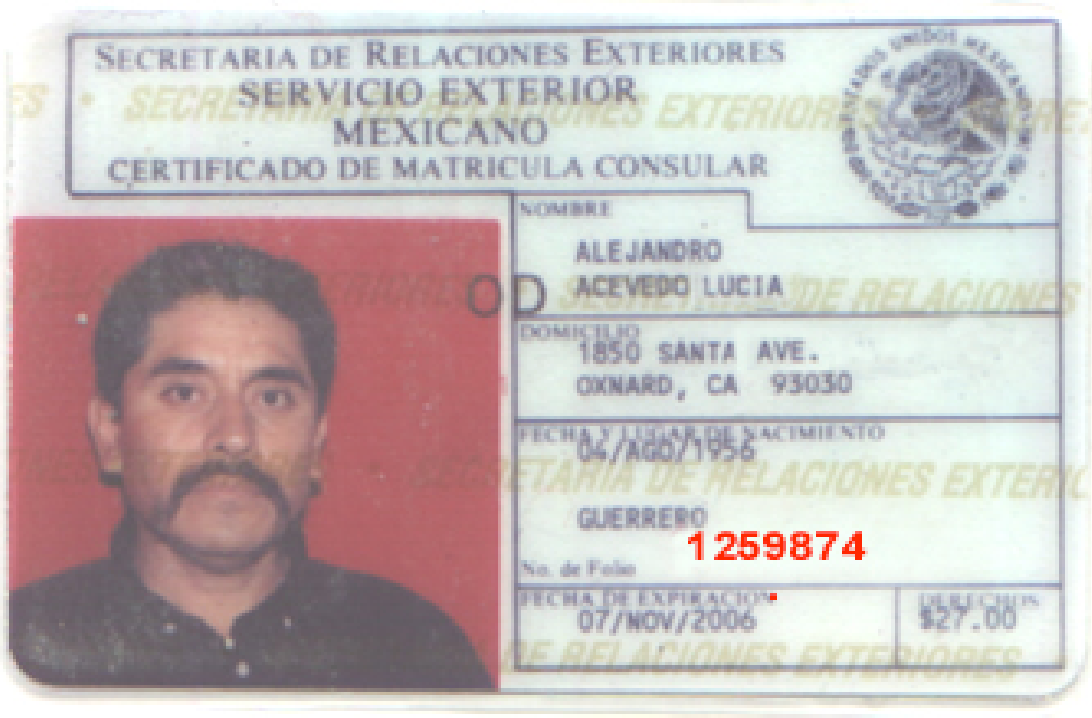
(what, you don’t trust foreigners?)

or this one?



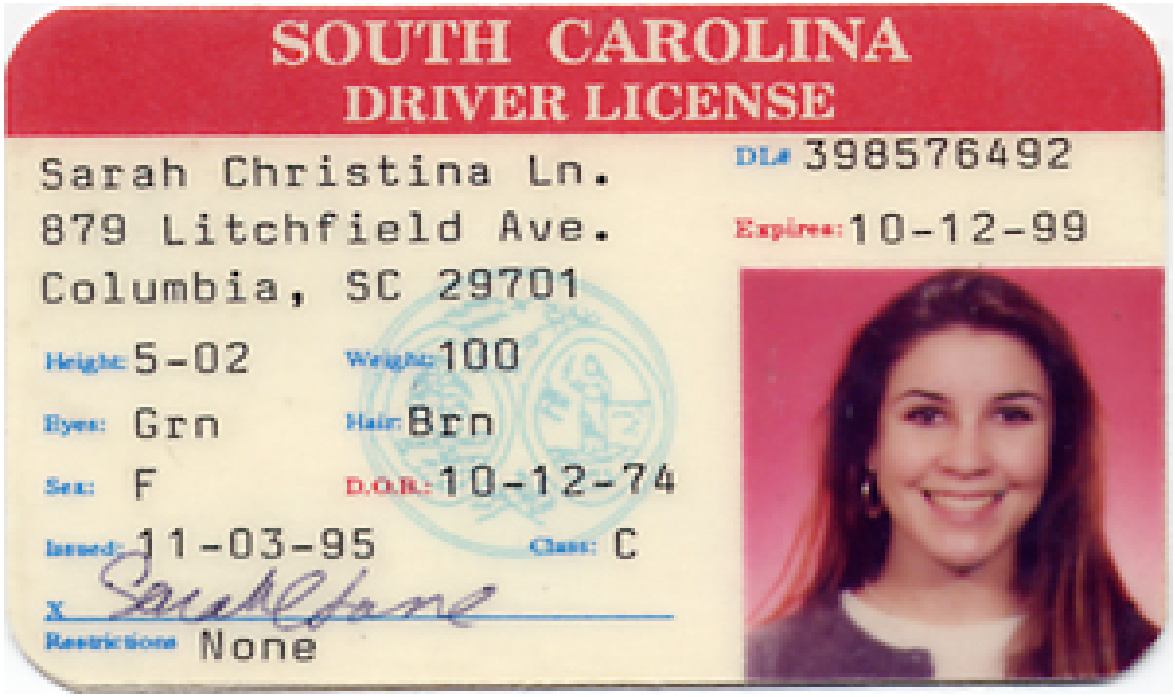
(people from the southwest probably see this one a lot more)

or this one?



(a variation on the same theme)

yeah, you can’t go wrong with photo id.



what’s wrong with this picture?

identity verification: a real person

just another average person…

a photo id gives out many details…

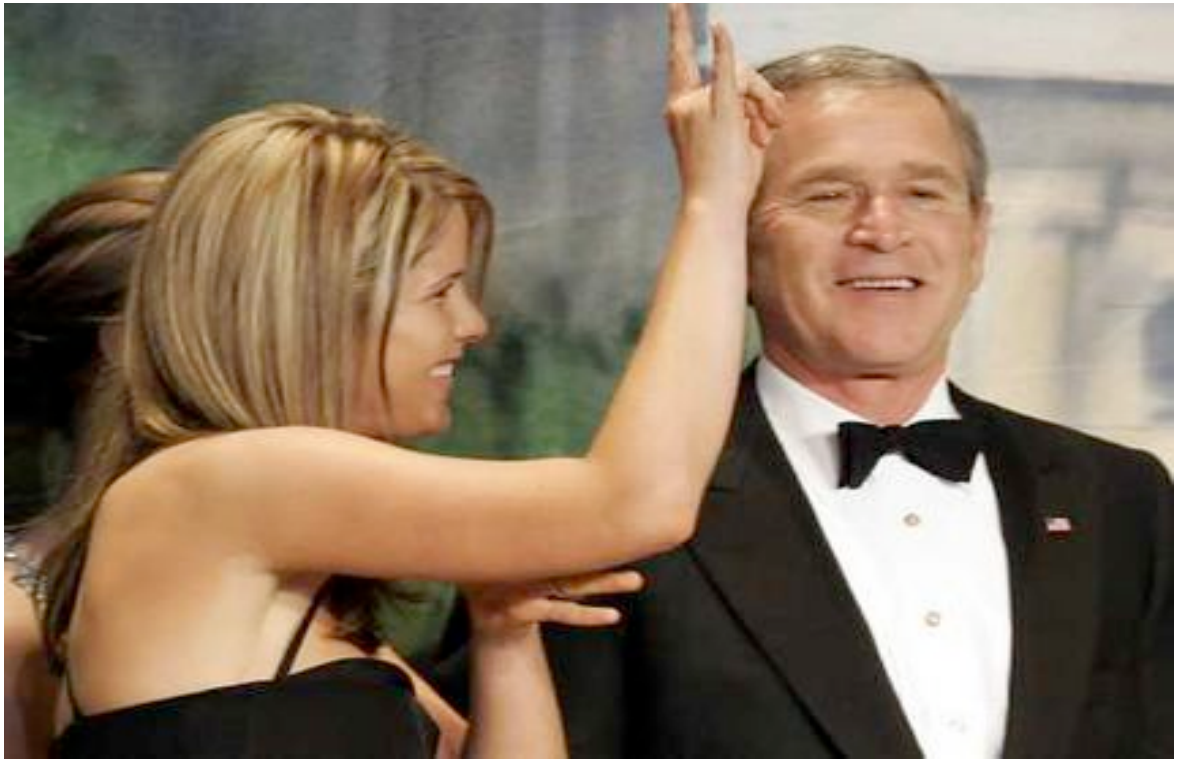
her name?

her address?

a photo id gives out many details…

why does she look familiar?

a photo id gives out many details...



here’s a picture of her and her father!

the point?

- do you know what a driver's license from south africa looks like?
- how good are you at spotting fake ids?
- do you want to be limited to signatures only from your own geographic region?
- how does a photo id *prove* someone's identity?

identity verification without an id?

- what if someone refuses to show id?
- what if the name someone goes by (and is on the key) does not match what is on the id?
- should people who go by pseudonyms or handles, and paranoid people in general be excluded?

verifying a handle is impossible.

who is this person?

verifying a handle is impossible.

how about this guy?

uids are for human convenience

- a uid on a key binds identity information to key information.
- does it matter whether you're talking to "seth hardy" or "shardy" as long as you know you're talking to the right person?
- some people are known a lot better by their pseudonyms...

uids are for human convenience

- *a uid on a key binds identity information to key information.*

- why do people restrict what identity information they'll verify?
- photo uids are accepted, but i've never seen a phone number as a key uid

time for some shenanigans!

[HOPE6 keysigning party shenanigans go here!]