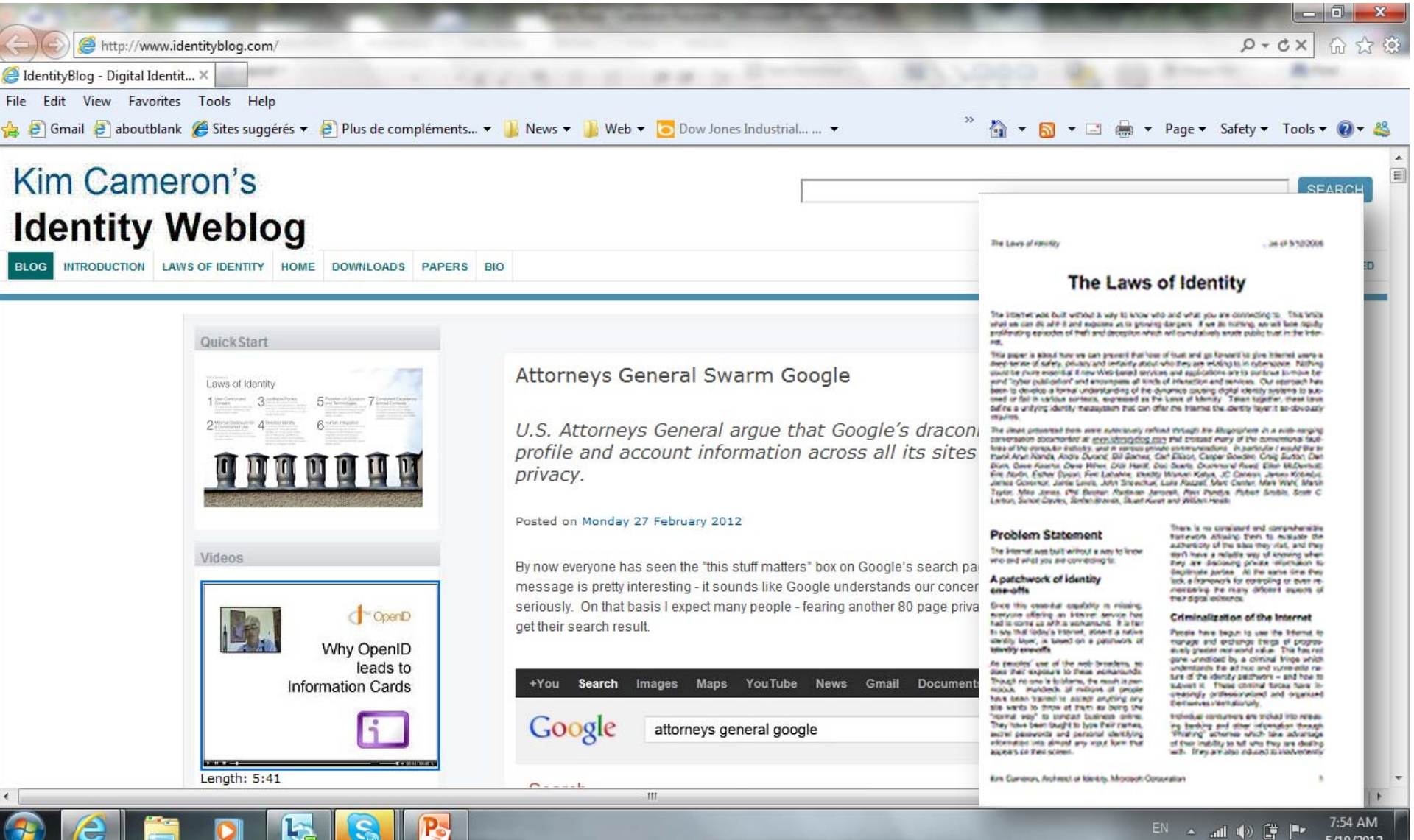
IDENTITIES AND FAKE IDENTITIES

Kim Cameron
Chief Architect of Identity
Identity And Access Division, Microsoft
http://www.identityblog.com

I'M A SOFTWARE ARCHITECT



WHAT IS IDENTITY?

1. The state or fact of remaining the same one or ones, as under varying aspects or conditions.
2. The state or fact of being the same one as described.
3. The individual characteristics by which a person or thing is recognized
4. The state of having unique identifying characteristics held by no other person or thing
5. The condition of being oneself or itself, and not another

MEDIEVAL LATIN
IDENTITĀS

SAMENESS, IDENTITY

ABSTRACTED FROM IDENTIDEM "OVER AND OVER," FROM PHRASE IDEM ET IDEM.

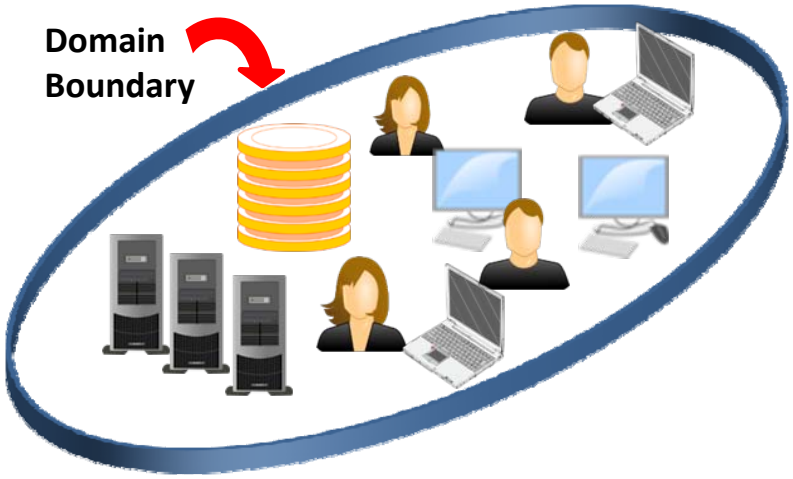
EMERGENCE OF IDENTITY IN MAINFRAME COMPUTING

- Tied to context and purpose:
  - Distinguish one computer user from another for purposes of safely running the computer and protecting privacy of users
- Began as no more than an identifier associated with a user (*identidem*) and verified manually when “jobs” were submitted to an “operator”
- Identifiers were used initially to control resource allocation and access, but by 1965 they were used in multiuser systems to provide boundaries between execution environments (privacy)
- Passwords were added when “self-service” and remote terminals were introduced to minimize likelihood of one user posing as another (*a secret held by no other person*)
- Information about users was not available to programs
- Emergence of paradigm of message-based systems and “the guard”

TIED TO PURPOSE OF RUNNING THE COMPUTER

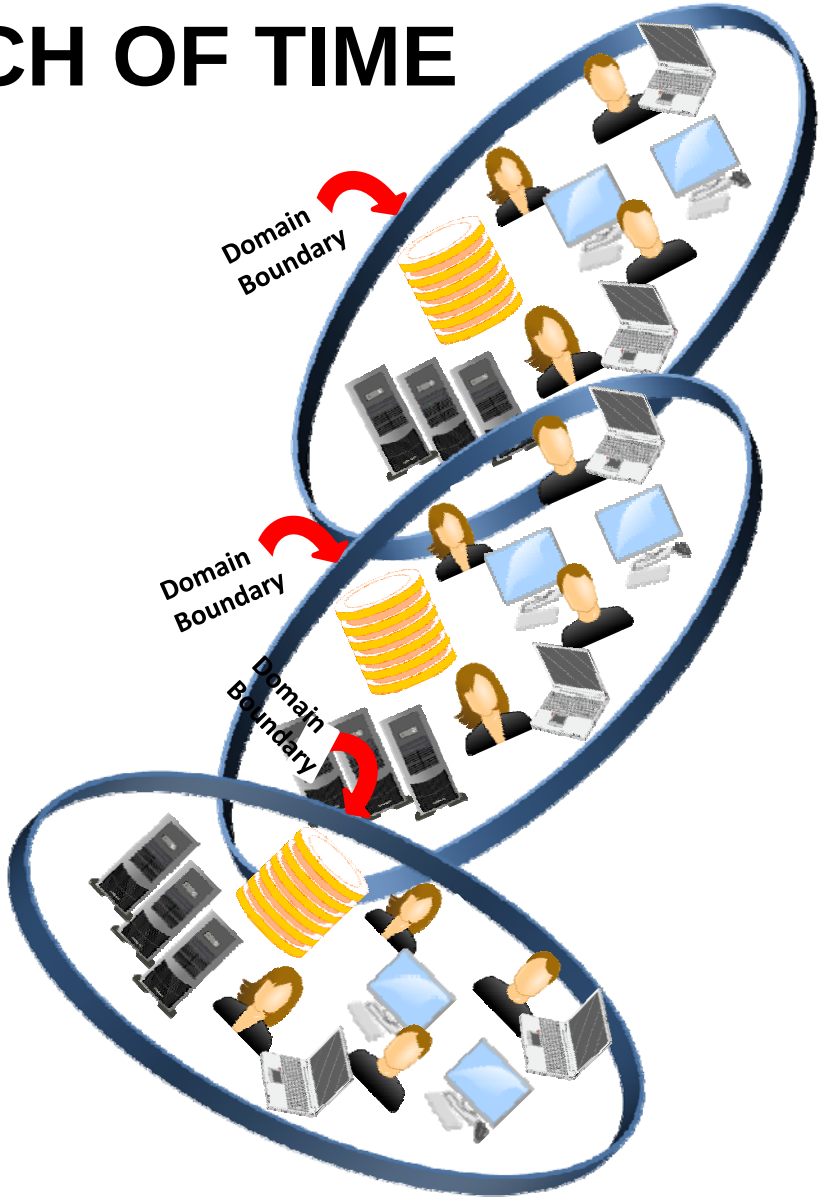
ROLE OF IDENTITY IN LOCAL AREA NETWORKS

- Again tied to context:
  - Distinguish computer users for purposes of safely running computers and protecting their data and privacy while allowing them to share resources on a network
- Concept of all-powerful domain
  - Molecular identities orthogonal to computer systems
  - Hermetic and self-referential
  - Central identity repository (directory or key distribution center) maps secrets to identifiers
  - Users prove knowledge of secrets, domain asserts the identifiers, domain entities trust them unconditionally

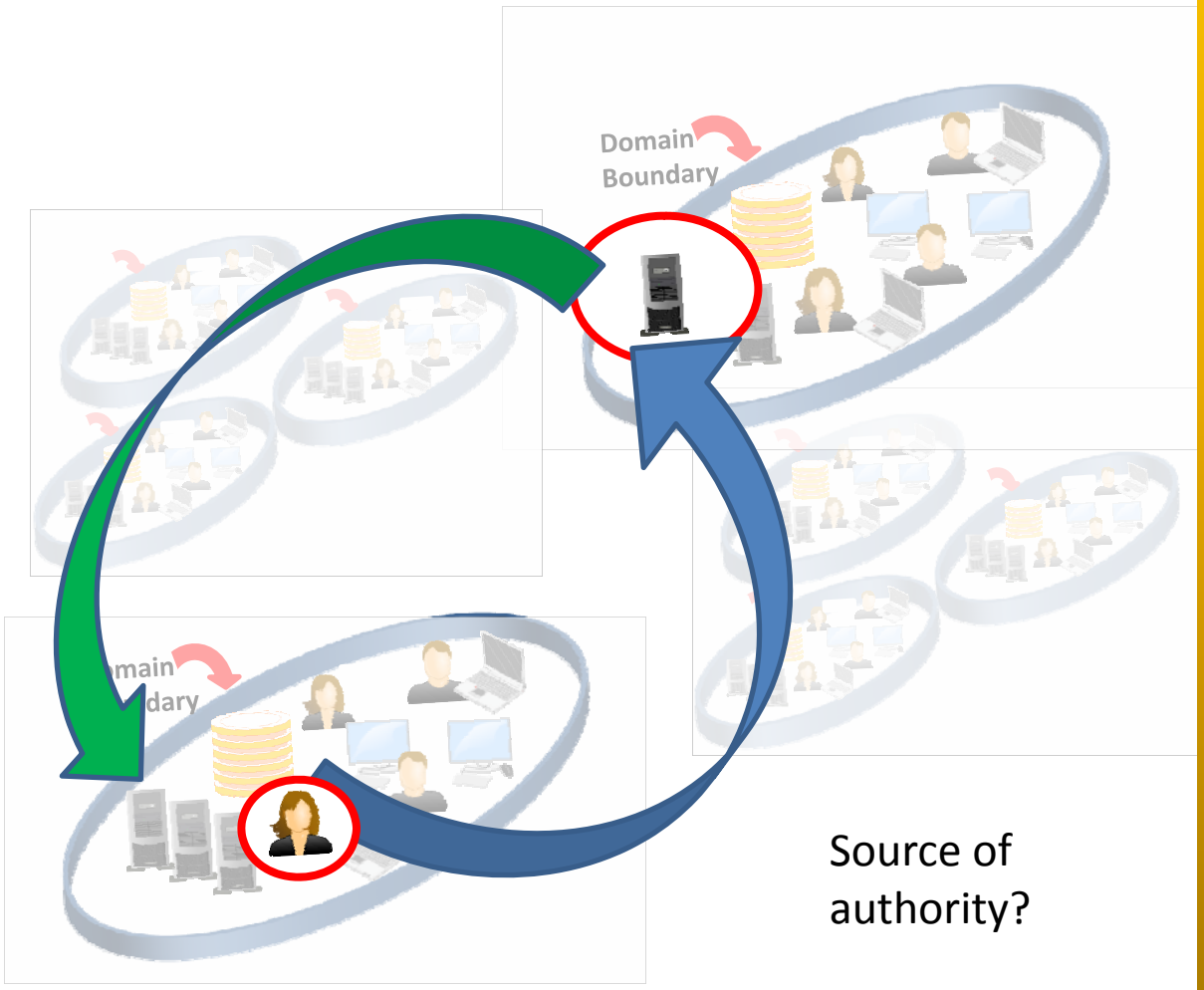


THE DOMAIN MODEL BESEIGED BY THE INTERNET AND MARCH OF TIME

- Many domains, many authorities, context unclear
  - Hermetic approach no longer realistic
  - No central identity repository as we cross domain boundaries
  - No simple model of unconditional trust
  - Identifiers have no universal meaning
  - No shared semantics or taxonomies
  - Bilateral trust models too complex and dangerous



AND BECOMES … UNWORKABLE



Source of authority?

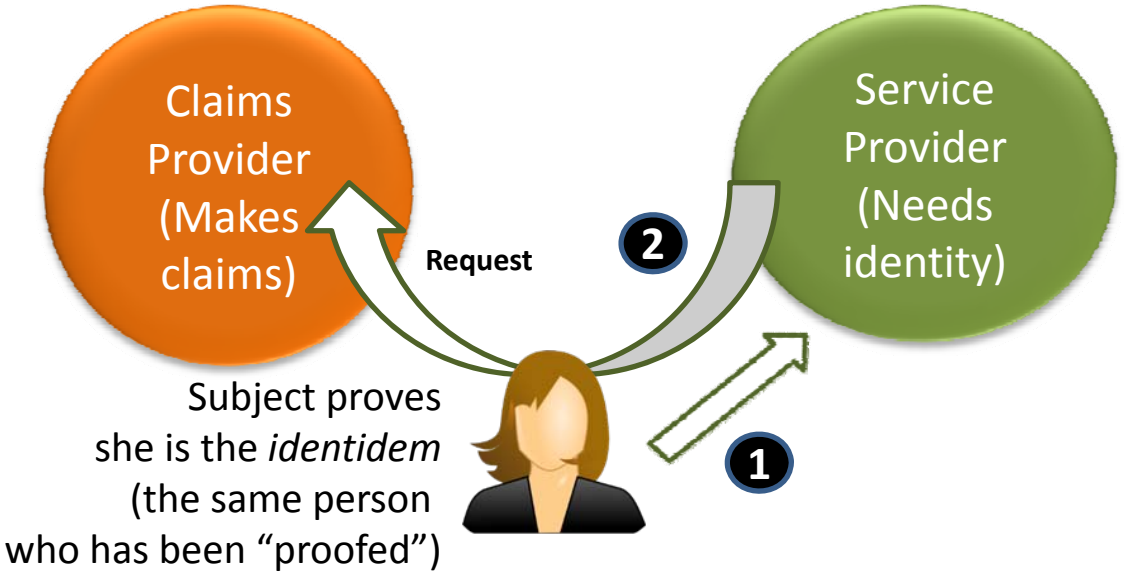
HOW DOES THE COMPLEX ACCESS CONTROL DECISION WORK ACROSS CONTEXTUAL BOUNDARIES?

SOLUTION:
THE CLAIMS BASED MODEL

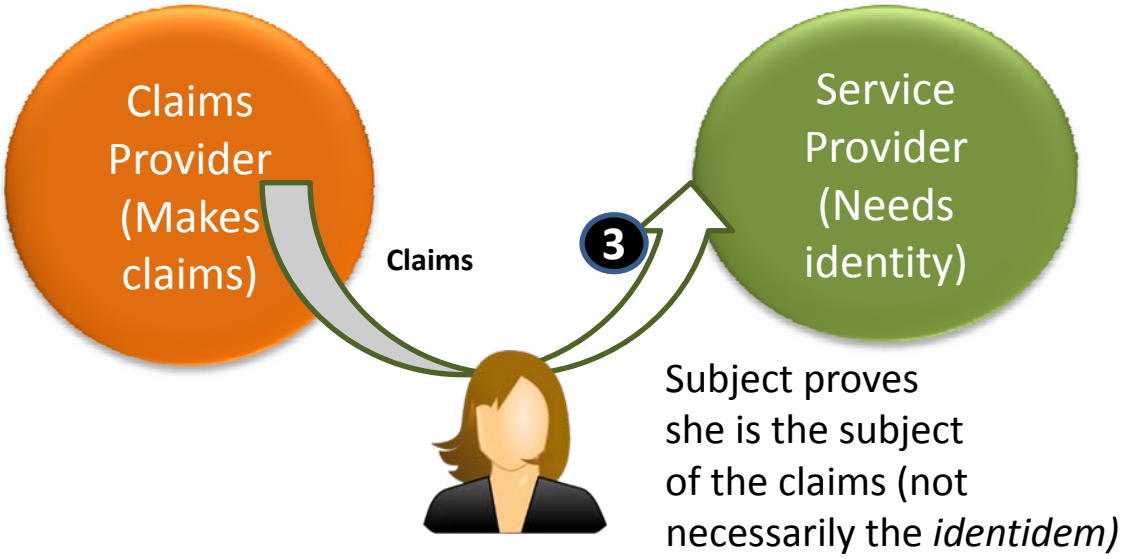
- A claim is something (anything) said by a “claims provider” about a “subject”.
- Examples: identifiers, names, attributes like age, derived claims like “over 21” or “citizen of the EU”, qualifications, capabilities
- Claims may apply to people, devices, contexts, things, resources, organizations and combinations thereof
- Claims are “in doubt” depending on who makes them and who receives them
- A Digital Identity is a cryptographically verifiable set of claims
- Proof of possession of the claim may use keys and biometrics produced through privacy enhancing technologies (e.g. U-Prove and biometric encryption)
- There will be an ecology of claims providers and service providers who consume the claims
- The claims based model supersets all previous identity models

A DIGITAL IDENTITY IS A VERIFIABLE SET OF CLAIMS

THE CLAIMS BASED MODEL (GETTING CLAIMS)



THE CLAIMS BASED MODEL (PRESENTING CLAIMS)

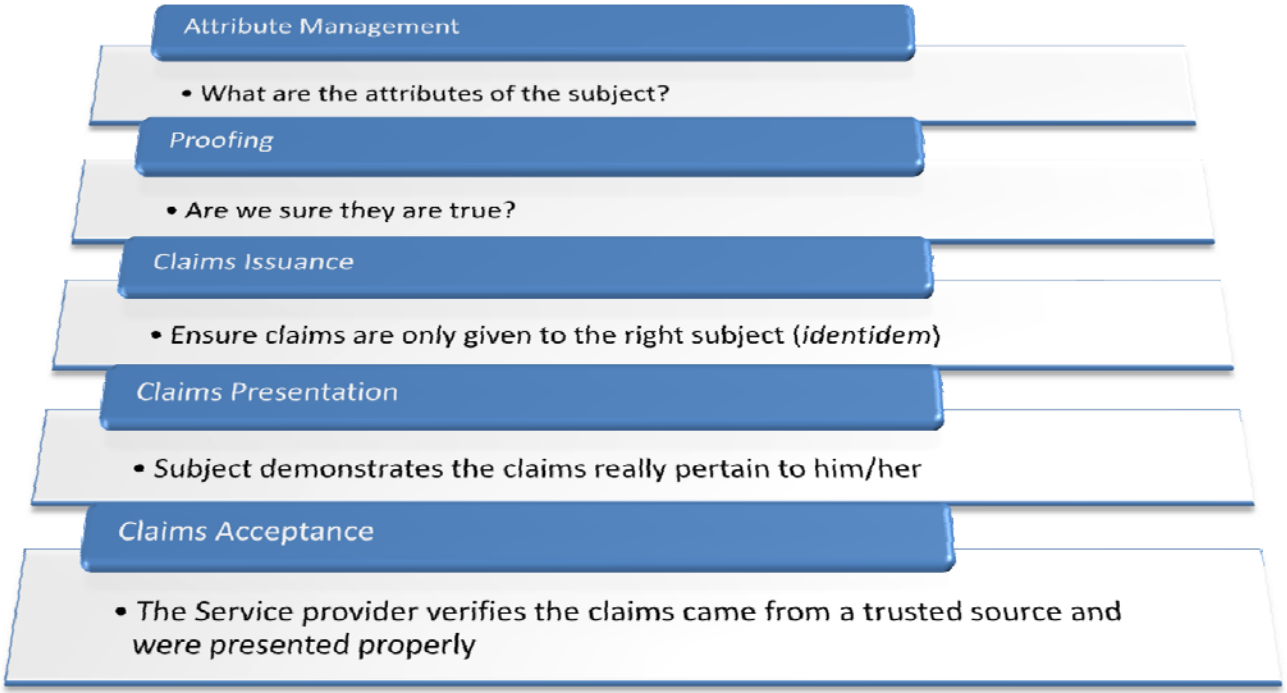


WORKS ACROSS CONTEXTS

- Allows contexts to be kept separate
- Allows contexts to be connected
- Supports “public” aspects of identity
  - “Omni-directional” claims
- Supports private identity relationships
  - “Uni-directional” claims
- Supports plurality of operators within a single technological framework

REQUIREMENT OF CONTEXTUAL SEPARATION IS FUNDAMENTAL TO USER EXPECTATIONS

THE CLAIMS LIFE-CYCLE – SERVICES NEEDED FOR CLAIMS TO WORK



WHY THE CLAIMS BASED MODEL OUTPERFORMS THE DOMAIN PARADIGM

Domain based model

- Single domain asserts subject's identifier
- Subject provides identifier to relying parties
- Relying parties must consult domain to obtain subject's attributes from identifier
- Subject has a universal identifier* linking activities
- Results in massive privacy issues

Claims based model

- Multiple claims providers asserts claims directly
- Subject conveys claims to relying parties
- Subject uses crypto or bio to prove claims pertain to him/her
- No universal identifier links the subject's activities
- Substantial reduction in privacy issues

FAKE IDENTITIES AND CLAIMS

What is “fake”

- Designed to deceive or cheat
- Not “real”
- “Counterfeit”.
  - made in imitation so as to be passed off fraudulently or deceptively as genuine; not genuine; forged
- “Anything made to appear otherwise than it actually is”

What is a fake identity

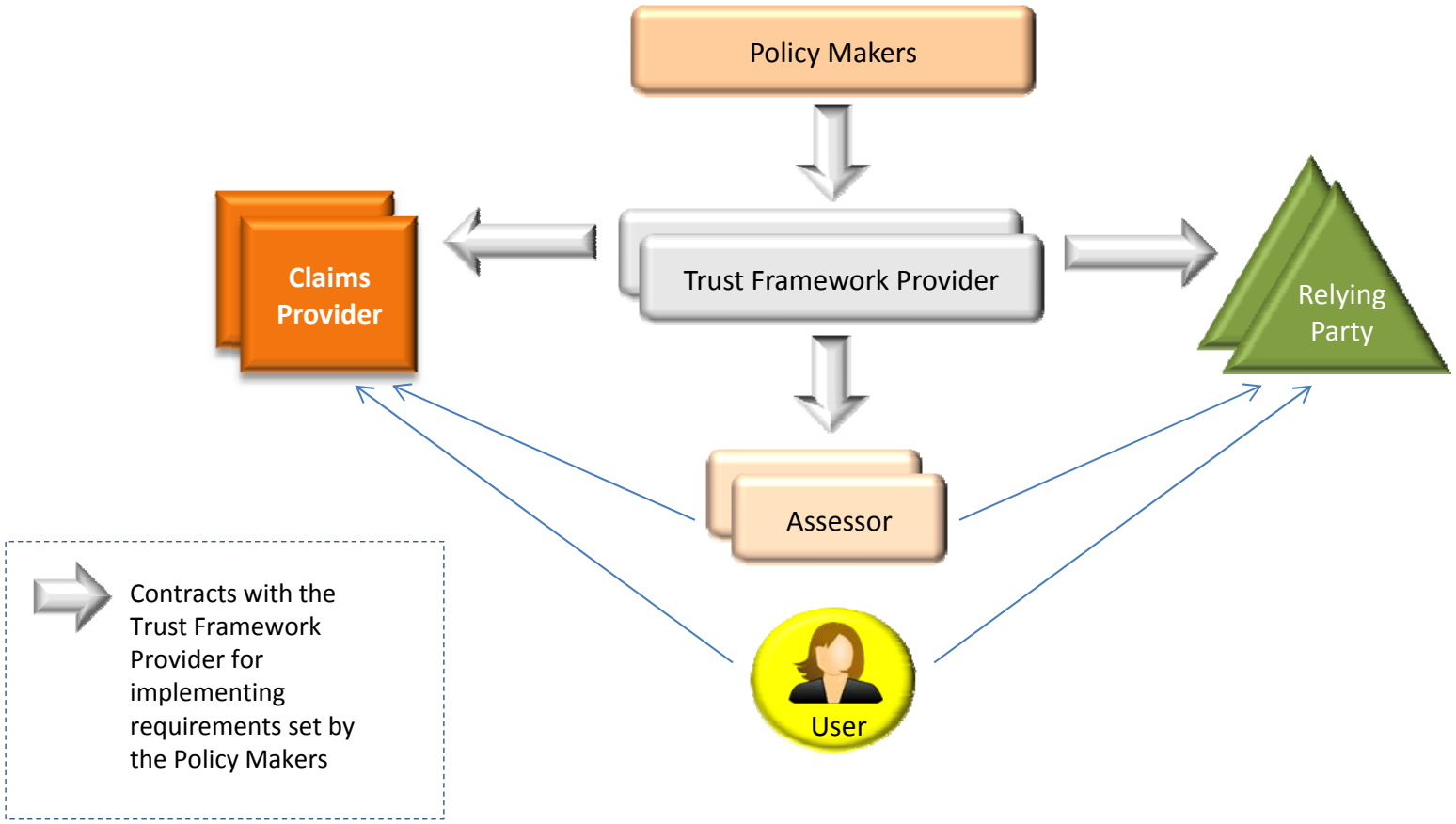
- Claims about the subject based on attributes that are untrue (e.g. false name, age, nationality, etc)
- Claims not really made by the entity claiming to issue them
- Claims legitimately made about one subject but presented by another (stolen claims)
- Claims made by an entity that is not trustworthy

What is “not fake”

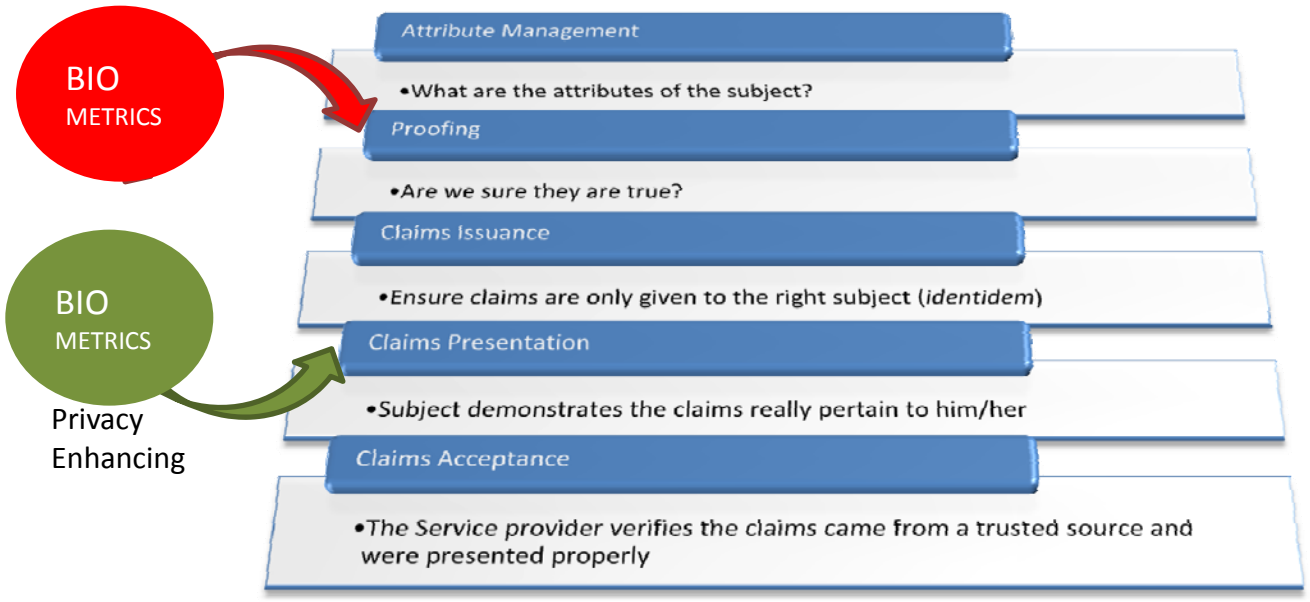
- Claims not specifying a “natural person” (Example of IdentityWoman)

ATTACK VECTORS IN CREATING FAKE IDENTITIES

MITIGATION: TRUST FRAMEWORKS



IN THIS WORLD TWO FUNDAMENTALLY DIFFERENT ROLES FOR BIOMETRICS



CONFLATING PROOFING AND PRESENTATION LEADS TO FEAR AND PANIC

One in three secondary schools fingerprinting pupils as Big Brother regime sweeps education system

By LAURA CLARK
UPDATED: 15:17 GMT, 9 June 2010

Comments (28) | Share +1 0 Tweet 0 Like 391

One in three secondary schools is forcing children to swipe their fingerprints just to register in class or take out library books, it emerged yesterday.

Figures diclosed under the Freedom of Information Act show how 'Big Brother' technology is becoming widespread in schools.

Thirty per cent of high schools are taking fingerprints simply to speed up basic administration such as borrowing books, registering in the mornings and buying canteen lunches.

Crackdown: One in three secondary students will be forced to submit an electronic fingerprint in order to carry out basic administration at school

The Telegraph

HOME | NEWS | SPORT | FINANCE | COMMENT | BLOGS | CULTURE | TRAVEL | LIFESTYLE
UK | World | Politics | Obituaries | Education | Earth | Science | Defence | Health News
USA | US Election 2012 | Asia | China | Central Asia | Europe | Australasia | Middle East

HOME » NEWS » WORLD NEWS » EUROPE » EU

Europe tells Britain to justify itself over fingerprinting children in schools

The European Commission has demanded Britain justifies the widespread and routine fingerprinting of children in schools because of "significant concerns" that the policy breaks EU privacy laws.

The commission has taken up the case of a father who has battled education authorities because his daughter's fingerprints were taken without permission Photo: ALAMY

By Bruno Waterfield, Brussels
9:30PM GMT 14 Dec 2010

Follow 4,727 followers

The commissioner is also concerned that parents are not allowed legal

Print this article
Share 757
Facebook 632
Twitter 120
Email
LinkedIn 5
+1 0

EU
News » World News » Europe » Bruno Waterfield »

IN EU

USE OF BIOMETRICS WITHIN DEVICES FOR PRESENTATION MEETS WITH SUCCESS

Microsoft unveils Avatar Kinect with facial recognition

Latest move in motion capture technology

By **Dean Wilson**

Tue Jul 26 2011, 13:24

SOFTWARE OUTFIT Microsoft has released a highly anticipated feature for its motion capture device called Avatar Kinect, which further enhances the Xbox 360's ability to display exactly what you're doing.

Avatar Kinect adds some of the functionality of the Nintendo Wii's Mii feature, but goes beyond simply displaying a caricature of who you are by allowing full body capture, and, even better, full facial recognition.

The Kinect can already capture full body movements, which is useful for dance games and similar titles, but capturing the nuances of a person's facial movements is an entirely different ball game.

Avatar Kinect can track the movements of a person's head, their mouth, and their eyebrows, giving a very impressive digital rendition of what they look like and what they are doing as they speak. It does not track more subtle movements like blinking or facial twitches, but it's certainly enough to get a hint of emotion from the person behind the avatar.

Users will be able to play around with their avatars in one of 24 virtual stages, with up to eight people present on screen at any one time. You can create a chat show style environment, which could spice up normal group chats between friends

How **Facial Recognition** Works in Xbox **Kinect** | Gadget Lab | Wired ...
www.wired.com/.../how-**facial-recognition**-works-... - Traduire cette page
5 Nov 2010 – Microsoft's $150 Xbox add-on, the **Kinect**, can use face-**recognition** technology to log you onto your Xbox Live account. But it's not trouble-free.

Kinect Sign In | Xbox Automatic Sign In | **Kinect** ID - Xbox.com - Xbo...
support.xbox.com/**kinect**/setup-and.../auto-sign-in - Traduire cette page
Find out how to teach **Kinect** to recognize your face and automatically sign ... **Kinect** ID remembers your previous sessions and improves **recognition** each time it is run. ... If you change your hairstyle or **facial** hair, set up your **Kinect** ID again.

Apple's iOS **facial recognition** could lead to **Kinect**-like interaction ...
www.reuters.com/.../idUS342371426620110727 - Traduire cette page
27 Jul 2011 – Apple has included **facial recognition** technology in iOS 5, 9to5Mac discovered earlier this week. It's not something Apple is advertising about ...

BACKDROP: FALLOUT FROM "OUT-OF-CONTROL" BIOMETRICS

Facebook Turns On Facial Recognition For Tagging By Default

June 08, 2011 by **Brenna Ehrlich**

60

If you have a bunch of tag-happy Facebook friends, you may want to read this. Facebook has been rolling out a facial recognition feature that makes it easier to tag friends in snaps, and it has introduced this feature as a default setting.

We first heard about Tag Suggestions back in December.

FOLLOW THE LAWS OF IDENTITY

Kim Cameron's

Laws of Identity

1 User Control and Consent
Technical identity systems must only reveal information identifying a user with the user's consent.

2 Minimal Disclosure for a Constrained Use
The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.

3 Justifiable Parties
Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.

4 Directed Identity
A universal identity system must support both "omni-directional" identifiers for use by public entities and "uni-directional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

5 Pluralism of Operators and Technologies
A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.

6 Human Integration
The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.

7 Consistent Experience Across Contexts
The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.