An introduction to the 3rd epoch of IDTrust

Ian Glazer
Research Director, Gartner
@iglazer - ian.glazer@garter.com

Well, how did we get here?

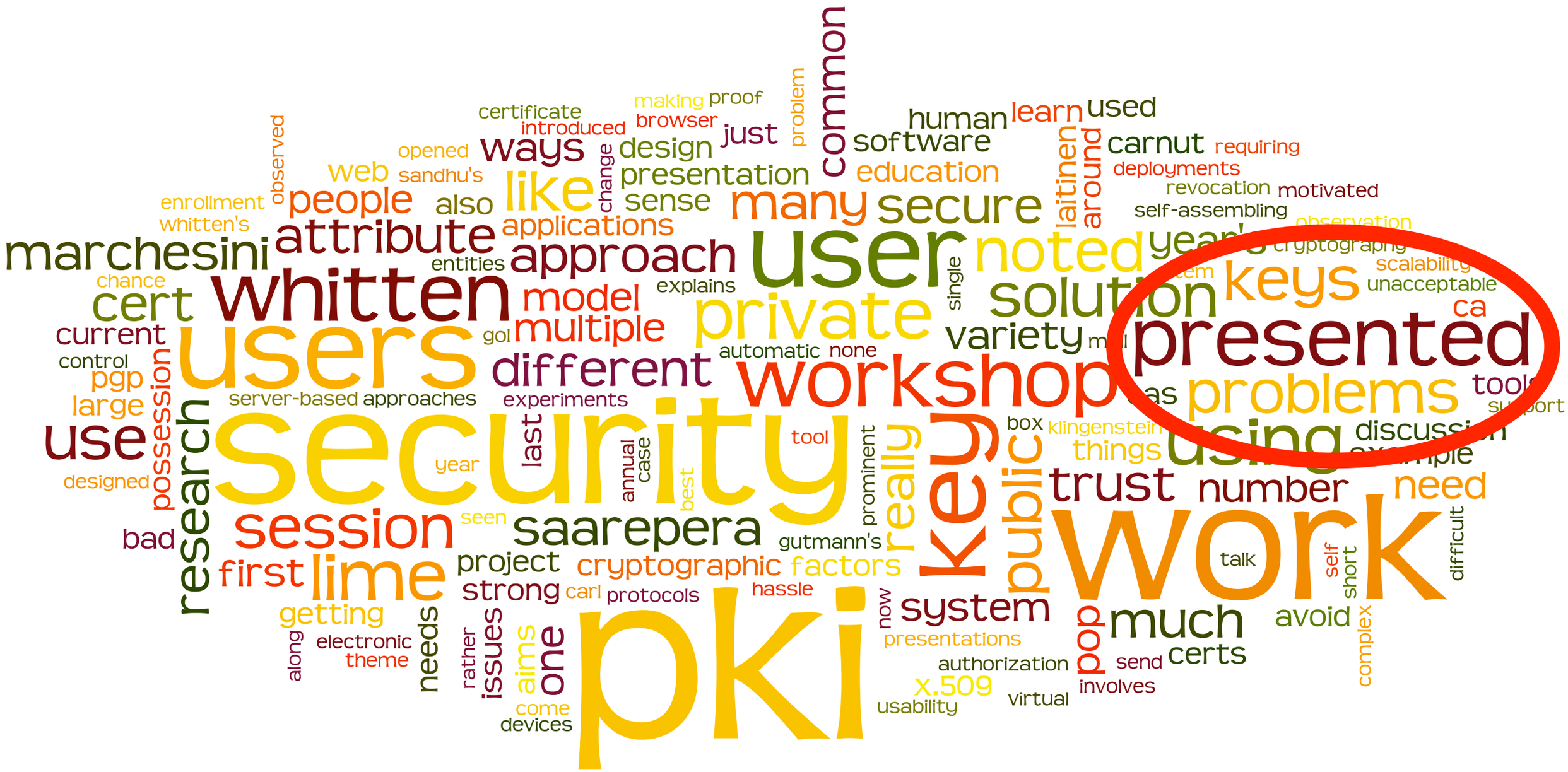
3 Epochs

Epoch 1: PKI

2002 - 2007

Annual PKI Research Workshop

overview
hierarchical
provide
example
akenti
carl
usually
geneva
better
appropriate
many
department
infrastructure
research
sufficiently
emphasized
top-level
existing
noted
work
questions
card
one
ensure
social
tends
practitioners
convention
collaboratory
central
variety
management
organizations
lines
x.509
order
internet2
discussed
readers
pointed
described
awareness
key
issues
user
distributed
boneh
used
uses
possible
need
included
tokens
sender
keys
main
wide
two
real-world
rather
green
provided
experts
complexity
observed
base
spki
get
certificates
mobility
needs
taking
ibe
go
area
sandhu
levy
built
much
report
follow
also
assumption
cryptography
micali
legal
use
validity
aka
set
public
makes
principal
private
approaches
non-hierarchical
authority
deployment
bridge
dealing
current
naming
ellison
server
time
credit
alterman
directory
agreement
pkis
policy
strong
collaborative
workshop's
certificate
someone
hallam-baker
traditional
presentations
want
encryption
passwords
peter
starting
smartcard
developed
conventional
discussion
sense
dohrmann
addition
sufficient
annual
authorization
system
security
work
shop
experience
validation
technical
Text
relationships
PKI



security
pki
work
users
user
workshop
presented
keys
problems
using
public
key
private
whitten
marchesini
attribute
approach
model
multiple
different
session
saarepera
lime
first
cryptographic
factors
system
much
trust
number
need
people
like
many
secure
noted
solution
variety
common
software
education
presentation
design
ways
just
certificate
introduced
making
proof
browser
human
learn
used
carnut
requiring
deployments
revocation
motivated
self-assembling
observation
cryptography
scalability
unacceptable
ca
tools
support
discussion
example
things
box
klingenstein
tool
prominent
really
gutmann's
hassle
protocols
carl
strong
project
seen
best
annual
case
last
year
gol
explains
entities
applications
sense
also
web
sandhu's
opened
observed
enrollment
whitten's
chance
cert
current
control
pgp
large
use
possession
research
designed
bad
getting
along
electronic
theme
needs
rather
issues
aims
one
come
devices
now
presentations
authorization
x.509
usability
virtual
involves
send
certs
pop
avoid
complex
self
short
talk
difficult
single
automatic
none
server-based
approaches
experiments

lessons
used
session
without
six
one
parties
electronic
usually
guida
digital
consensus
credentials
dynamic
stillson
government
klingenstein
project
pointed
three
action
observed
challenge
response
now
federal
peter
requirements
know
various
real-world
driven
brands
hesse
standards
plan
gutmann
delegation
become
make
data
test
users
way
things
trust
relying
authorization
along
put
new
everyone
research
get
must
transactions
path
much
different
take
use
bridge
even
often
like
rather
particular
work
discussion
privacy
deployment
key
polk
main
years
anything
certificates
stressed
issues
suggested
technology
two
big
certificate
first
also
web
rights
xrml
time
focus
possible
trusted
hanna
ellison
user
needs
understanding
e.g
problem
factors
areas
application
atient
pgp
using
needed
applications
described
security
need
tools
workshop
importance
many
system
meeting
choices
approach
sessions
variety
building
presented
name
global
question
approaches
process
groups
human
proposed
validation
tasks
people
x.509
getting
experiences
paper
group
vendors
adams
technical
lawyers
public
order
panel
steve

pki
also
note
presented
approach
work
security
discussed
deployment
workshop
signatures
standards
cross-certification
one
user
session
particular
year
fips
move
much
need
access
deployments
several
secure
area
needed
two
ietf
just
group
cards
trust
attacks
research
contactless
new
issues
bof
make
like
control
ongoing
still
expected
considered
enrollment
including
nielsen
ibe
aimed
government
callas
shibboleth
polk
roles
acceptable
requirements
trials
developments
safe
agreement
general
lead
key
wip
see
interoperability
e.g
system
certificates
privacy
guida
getting
hardware
healthcare
legal
use
x.509
support
delegation
papers
digital
federal
many
garfinkel's
time
yet
usable
end
advantages
move
discussion
focus
offering
care
pointed
likely
projects
related
phinms
problem
consensus
authentication
lot
hci
standard
smartcards
replacement
principle
reducing
application
norman
list
paper
important
technical
community
agreement
generally
around
ways
involved
housley
making
zagar
major
nist
well
strong
cryptography
eric
presentations
obstacle
working
applying
analysis
described
management
certs
underway
companies
pki03
based

also
needed
security
deployment
dkim
users
pki
signatures
noted
trust
user
see
signing
discussion
work
discussed
use
software
presented
suggested
interface
like
chadwick
solution
panel
key
sasse
certificate
approach
grid
burr
email
using
things
get
stressed
domain
presentations
management
whitten's
better
way
gave
europe
paper
browser
know
used
rather
make
hebca
rundgren
provided
sean
cited
validation
order
globus
identity
talk
bridges
pockets
nist
internet
strongly
project
dnssec
constraints
time
digital
involved
chokhani
va
shibboleth
one
secure
much
processes
argued
among
services
list
technical
moderated
transactions
want
usability
good
experiences
short
requiring
well
based
focus
uses
standards
expect
strong
signature
standard
best
major
suite
complex
available
kerberos
working
practices
relying
interoperability
education
pki06
patent
system
design
workshop
higher
holt
include
program
many
emphasis
particular
just
david
ecc
herzberg
revocation
components
yiu
advocates
training
bad
now
web
two
support
overview
federal
example
cryptography
new
around
credentials

2007

identity
system
authentication
technical
rump-session
bacchus
creating
trust
service
advanced
piv-enabling
parties
electronic
year
security
uk
universal
approaches
agreement
identities
much
uses
signing
consistent
technologies
interest
e.g
short
project
hspd-12
concerned
business
x.509
means
passports
providers
documents
federations
current
things
cantor
work
grid
use
gave
web
talks
relying
human
using
used
layer
just
among
aspects
data
need
pki
ca
internet
information
government
every
workshop
census
certificates
applications
stressed
see
noting
panel
via
made
working
introduced
presented
mortgage
discussed
digital
infrastructure
including
years
klingenstein
public
kerberos
many
privacy
management
attributes
way
key
signatures
like
mcintosh
federal
planned
authorization
submissions
user
also
limited
industry
far
time
two
cameron
education
shibboleth
identifying
jensen
paper
implementation
must
four
piv
rather
point
general
currently
variety
problem
single
users
expected
higgins
delegation
october
treasury
great
common
particular
developed
passwords
entities
saml
access
leblanc
process
described
three
one
ellison
metasystem
approach

Epoch 2: Identity

2008 - 2011

Symposium of Identity and Trust on the Internet

information
access
authentication
system
encryption
certificate
security
identity
user
key
pki
user
certificates
service
data
server
policy
network
control
backup
private
scheme
management
ipf
section
secure
must
based
technologies
used
digital
public
encrypted
symmetric
application
trusted
different
work
accreditation
attribute
skms
openid
internet
components
algorithm
available
design
given
servers
set
another
encrypt
step
device
machine
credential
client
keys
also
new
protocol
architecture
systems
type
example
needs
technology
support
however
may
auditors
like
end
specific
site
decrypt
single
without
allows
credentials
sites
order
figure
two
well
account
secret
storage
time
cards
approach
process
documents
hsm
applications
revocation
multiple
cryptographic
number
within
database
since
sensitive
issued
many
ca
relationship
policies
attributes
configuration
store
make
sks
every
able
provider
see
need
one
provide
web
cas
request
services
card
records
signed
way
software
users
document
token
frastructure
stored
first
possible
schemes
xri

key
trust
user
identity
certificate
management
information
public
credentials
credential
access
security
authentication
service
users
used
issuer
systems
provide
may
need
pki
nasa
keys
card
number
one
using
message
transaction
provider
authorisation
email
order
secure
section
trusted
path
protocol
based
certificates
private
time
ca4
support
belief
gnupg
certification
messages
different
risk
digital
paper
ca
services
secret
application
process
multiple
software
aggregation
infrastructure
system
federal
approach
ca3
framework
signed
subject
sharing
usability
new
given
capabilities
current
user's
receipt
data
td
problem
make
relationships
work
re
protocols
degree
first must
organizations
control
distrust
specific
network
example
sp
authorization
spici
alice
group
tpse
level
required
piv
agency
business
attributes
encryption
needed
paths
however
assurance
encrypted
two
single
study
policy
figure
related
way
lists
value
server
scheme
i.e
mobile
since
verification
able
also
set
part
attribute
well
se
chain
provides
model

identity
content
trust
provider
policy
user
key
information
data
use
section
access
certificate
teragrid
authorization
authentication
number
protocol
system
security
used
scheme
anchor
policies
using
management
store
box
service
token
message
attribute
biometric
different
users
browser
federated
secret
since
digital
figure
without
campus
results
given
request
set
node
mod
particular
may
cardspace
certificates
pks
work
one
via
required
address
might
constraints
case
applications
account
provides
classes
federation
integration
approach
blind
order
re
list
application
ing
rp
need
first
part
paper
bid
make
table
pca
well
idp
single
providers
tion
attributes
model
image
time
also
based
proposed
available
severa
privacy
reference
whether
party
possible
pki
anonymous
two
web
keys
must
saml
support
able
alice
example
requires
network
values
verification
cash
structure
current
multiple
ta
page
capi
hash
provided
public
liberty
specific
process
however
value
algorithm
target
described
extension
identities
sections

identity
management
security
attributes
biometric
issues
sector
public
privacy
technologies
attribute
ecosystem
look
strategy
key
authentication
information
systems
system
development
landscape
years
individuals
statement
identifier
organizations
challenges
standards
marketplace
cyberspace
normalization
different
emerging
policies
cases
implementation
schema
biometrics
authority
since
assurance
access
nist
just
show
typically
least
lead
jeremy
consequence
trusted
private
federated
session
government
resources
statements
e-authentication
discuss
advocacy
essential
developed
consumption
number
debates
discovery
testing
including
play
house
pharmaceuticals
particular
concepts
system's
role
noted
need
may
utility
i.e
several
needs
panel
consumer
openid
chains
single
balance
opening
experts
debate
new
air
also
countermeasures
desktop
higher
working
jurisdictional
technical
usability
services
control
white
retrospective
permissions
products
agencies
personal
grant
identities
users
algorithm
groups
algorithms
describes
technology
versus
whither
asked
give
normal
oauth
others
non-revocable
like
continues
focus
release
overall
becoming
communities
asking
advances
national
ensure
large
support
substantial
cross-protocol
calls
research
soon-to-be-released
successful
authenticators
financials
physical
transactions
resources

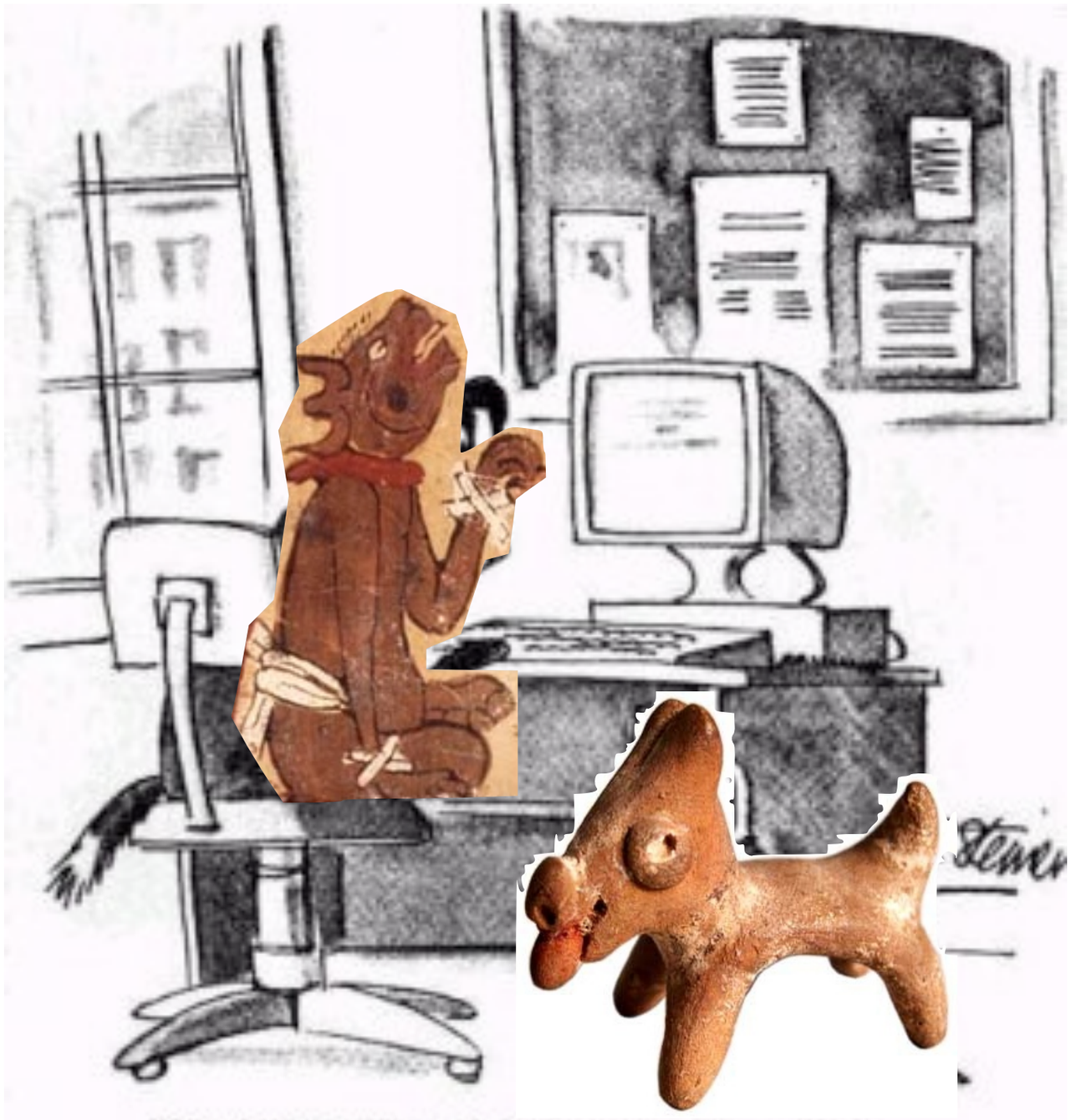
Epoch 3: Enabling the Identity Ecosystem

2012 - ?

2012

WE WERE WARNED
A ROLAND EMMERICH FILM
2012
NOVEMBER
FIND OUT THE TRUTH. SEARCH:2012

We better get to work



"On the Internet, nobody knows you're a dog."

Mayan

"On the Internet, nobody knows you're a dog."

2016

We better get to work

Epoch 3: Enabling the Identity Ecosystem

- Identity solutions will be privacy-enhancing and voluntary
- Identity solutions will be secure and resilient
- Identity solutions will be interoperable
- Identity solutions will be cost-effective and easy to use

Gaps and Challenges for Advancing the Global Identity Ecosystem

- Tom Smedinghoff
- John Bradley
- Ken Klingenstein
- Leif Johansson

Lucy Lynch
ISOC

Are Privacy Challenges Manageable?

If carried out close to its ultimate vision, the Identity Ecosystem will be composed of a huge, interlocked network of identity and attribute providers, relying parties, individual consumers and citizens, an unimaginable number of interdependent applications, services and devices, standards, and competing regulatory and audit requirements. In such an environment, **is it possible to have any assurance of privacy**? Are privacy risks understood and manageable?

John Sabo

Usability

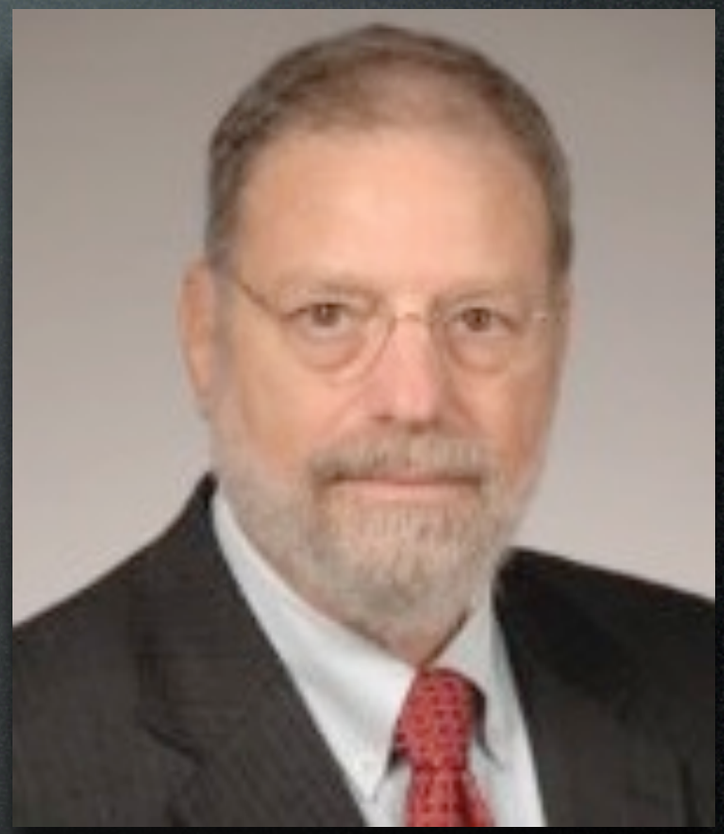
The usability panel panel discussions by leading identity management and standards experts addressing usability and the user experience in online banking, social media and ecommerce that surround identifying and implementing the four NSTIC Guiding Principles in the Identity Ecosystem:

- Identity Solutions will be Privacy-Enhancing and Voluntary
- Identity Solutions will be Secure and Resilient
- Identity Solutions will be Interoperable
- Identity Solutions will be Cost-Effective and Easy To Use

Don Thibeau

Where Trust Frameworks meet… or don't

- Mission
- Values
- Interoperability
- Governance



Peter Alterman

Searching for viable business models

- Tyler Moore
- Kaliya Hamlin
- Dave Coxe
- Peter M. Graham

Jeff Friedberg
Microsoft

Attributes & Attribute Providers

NSTIC departs from most earlier identity systems by identifying an ecosystem of attribute providers that is logically, if not operationally, separate from other identity providers. This raises a number of new issues, including the **standardization of attribute representations (schemata), business models for attribute providers, mechanisms for establishing trust in an attribute provider, and privacy issues**. This panel will examine the nature of these future attributes and attribute providers.

Jim Fenton

2016

Let’s get to work