The Quiet Enjoyment Infrastructure

Presentation to

NIST PKI-TWG

November 20, 2003

Wes Kussmaul

CIO, The Village Group

What is Quiet Enjoyment?

Quiet Enjoyment is the conveyed right to possess premises which meet a certain description, as in a lease or in a covenant, and to enjoy and use those premises in peace and without interference.

Quiet Enjoyment is the distillation of the terms of a lease into two words. It's what a landlord owes a tenant in good standing.

My Background in Real Estate

1981 Founded Delphi, “the world’s first online encyclopedia”

1982 Discovered that bars (real estate) are more profitable than libraries

1983 Discovered that office buildings are more profitable than bars or libraries

1986 Spun off The Village Group to build online real estate for *National Review*, *BioTechniques*, *Hardcopy*, *Business Review*, etc.

1993 Sold Delphi to Rupert Murdoch, who thought he was buying a library

What is a PKI?

An effective PKI is that which creates and maintains a bounded space in which people are able to pursue an agenda in Quiet Enjoyment.

Q: What is the difference between an effective PKI and a well-designed office?

A: Different construction materials.

Differences in construction materials imply other differences:

- Lack of visual and aural cues means you're not sure who's in the meeting room with you
- A 20,000 km tunnel is cheap to build
- Security guards may be robots
- The actual room may be copied as easily as the drawing is copied

Other differences not related to construction materials:

- Lack of building codes means property owners and tenants cannot be sure whether Quiet Enjoyment is being provided
- Commuting and parking should be a lot easier (the old telecommuting promises)

Given those differences, how do we get Quiet Enjoyment from our PKI?

- Compensate for lack of visual and aural cues with reliable identity credentials and with “indoor” technology
- Separate the identity credential from all other credentials
- Recognize that a tunnel is not a meeting room, much less an office suite
- Require occupancy permits

Quiet Enjoyment

What problems does PKI need to solve?

1. Enterprise Security
2. Keep The Internet from Falling Apart

How?

We Got It Right In The ’80’s with the

ID-PKI

What is the Quiet Enjoyment Infrastructure?

QEI is a PKI that

- Responds to *10 Risks* & other PKI critiques
- Builds on original Universal ID idea
- Proposes ID source with an important (often overlooked) ingredient
- Addresses Universal ID concerns with robust privacy protection
- Uses Real Estate metaphor throughout

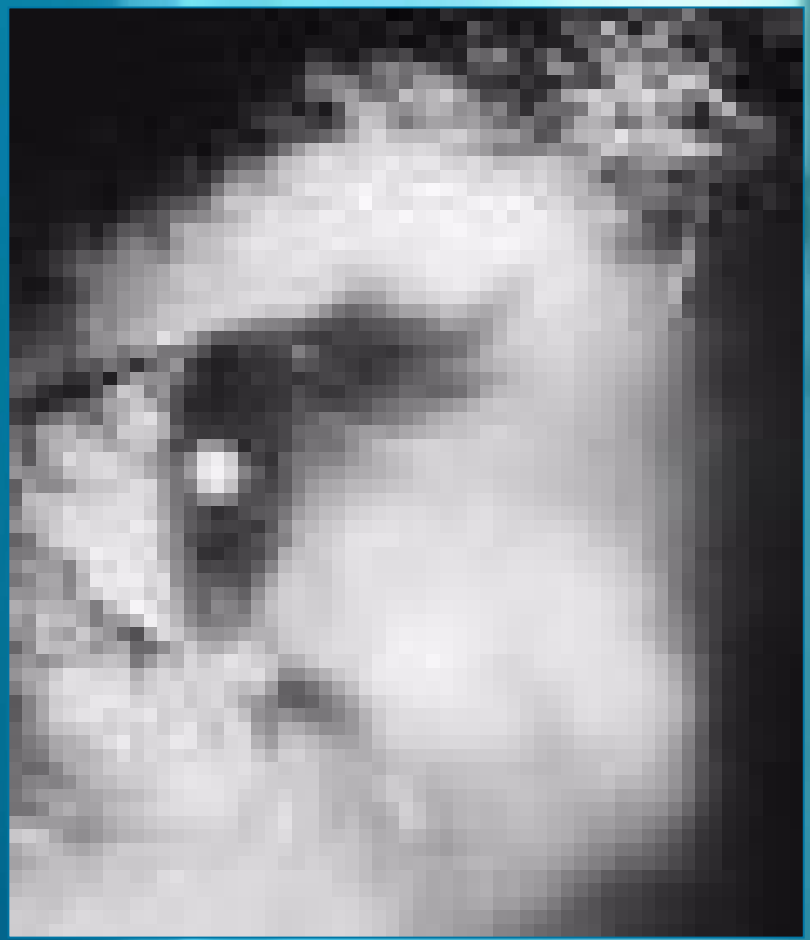
The PROBLEM

Today's VPNs are supposed to serve employees of suppliers, distributors, ad agencies, consulting firms, etc., etc.

Who issued their identity credentials? What good is an Identity Management System if the identities to be managed are of uncertain reliability?

***IDENTITY** is the **Foundation** of Security*™

The PROBLEM



Identity Crisis

For all the discussion of national ID cards and other identity tokens, none of the products, nor even the proposals, accomplishes the goal of strongly establishing identity.

The SOLUTION

The first step toward Quiet Enjoyment:

RELIABLE IDENTITIES

The Quiet Enjoyment Infrastructure consists of Twelve INSTIGATIONS

1. Local Crypto Infrastructure
2. Authority Infrastructure
3. Enrollment Infrastructure
4. Uniform Identity Infrastructure
5. Personal Intellectual Property Infrastructure
6. Law Enforcement Infrastructure
7. Building Codes Infrastructure
8. Indoor Operating System
9. Real Estate Professional Infrastructure
10. Media Industry Infrastructure
11. Public Roadways Infrastructure
12. Usable Vocabulary Infrastructure

Quiet Enjoyment Infrastructure / Instigation #1

Local Crypto Infrastructure

Part 1: Hard Token (“Wallet”)

- Multiple key pairs and other credentials
- One, two and three factor uses
- All signed by one foundational key

Part 2: Indoor Client

Examples:

- MS Palladium

(renamed “The Next-Generation Secure Computing Base For Windows”)

- Wave Systems’ Embassy Trust System
- TCPA
- Intel LaGrande
- Phoenix CmE
- “Sandbox” software-only approaches
- Others?

Quiet Enjoyment Infrastructure / Instigation #2

Authority Infrastructure

Q1: In a Certification Authority, where exactly does the Authority ingredient come from?

Q2: Do we really want to rely upon birth certificates, drivers' licenses and passports issued by commercial enterprises?

Q3: Is this the sort of thing that Matt Blaze was talking about when he noted that "A certification authority protects you from anyone whose money they refuse to take."

Q4: Where does authority come from, anyway? Where do we find this ingredient called fungible authority?

Q5: Isn't this the same question as "Where does government come from?"

Quiet Enjoyment Infrastructure / Instigation #2

Authority Infrastructure

A: Governments are sources of fungible authority.

- A good example: the Tabellione
- Another good example: the Latin Notary
- Yet another: the Indian Notary
- Horrible example: typical U.S. notary

The Authority Infrastructure uses Latin Notary standards as the basis for a worldwide standard for the practice of identity verification and credential issuance

Quiet Enjoyment Infrastructure / Instigation #2 & 3

Authority & Enrollment Infrastructures

- Face-To-Face (the only workable solution)
- Uniform Latin Notary Standards for Enrollment Officers
- Uniform Worldwide Procedures
- RA (Enrollment Officer) = CA
- RA = Liable party
- RA = Public Official
- (built-in criminal sanctions for malfeasance in office)
- $(E\&O)^2$
- Multiple Biometrics: Iris, Finger, Video with Voice
- Event stamped and signed from external sources

Enrollment Infrastructure

The VIVOS®

Enrollment Workstation

is a transportable integrated system of hardware and software that lets the certified authentication professional quickly and easily verify and record the identity of an individual and issue digital certificates and tokens in a number of forms.

Quiet Enjoyment Infrastructure / Instigation #4

Universal Identity Infrastructure

The Tabelio™ Birth Certificate is simply a birth certificate in X.509 form, with an asymmetric key length that is sufficiently long to stand up for a few years to the pressures of Moore's Law.

Quiet Enjoyment Infrastructure / Instigation #5

Personal Intellectual Property Infrastructure

Any attempt to implement a universal ID-PKI must be accompanied by a very strong answer to inevitable and valid privacy concerns.

PIPI puts teeth into the original P3P notion of letting individuals own and control PII.

Quiet Enjoyment Infrastructure / Instigation #6

Law Enforcement Infrastructure

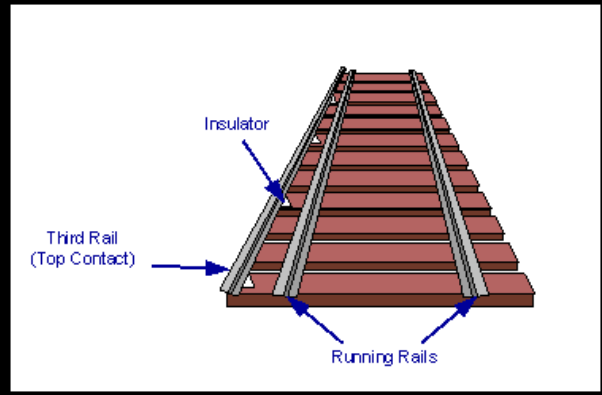
What about key escrow?

Should law enforcement have the ability to intercept encrypted communications?

Should that ability be maintained even in countries with oppressive governments?

Will any inter-net PKI plan survive if it does not address the concerns of law enforcement?

(Should I duck as I ask these questions?)



Quiet Enjoyment Infrastructure / Instigation #7

Building Codes Infrastructure

How do you know your building is secure and reliable?

Over millennia, people have discovered that the only adequate answer lies in public standards.

We call ours the Abyx standards.

Quiet Enjoyment Infrastructure / Instigation #8

The Indoor Operating System

What good is key management if the computer in which the key is used is vulnerable?

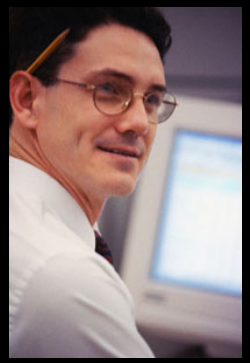
Highways are public outdoor spaces. That goes for information highways as well as physical ones.

The Osmium Standard applies to this Instigation as it does to the LCI Instigation.

Quiet Enjoyment Infrastructure / Instigation #9

Real Estate Professional Infrastructure

Addresses the software professional's dilemma:



@

HAD

Hidden Agenda Dynamics Incorporated

=

@

=

Quiet Enjoyment Infrastructure / Instigation #9

Real Estate Professional Infrastructure

The Real Estate Professional Infrastructure is strictly modeled after its physical counterpart. Occupancy permits are issued when a) the structure is built to code and b) the architect and contractors have been paid.

Quiet Enjoyment Infrastructure / Instigation #10

Media Industry Infrastructure

Q: Who's Going To Pay For All This?

A: Principal Relying Parties

Q: Who are they?

A: **Employers**

VPN Owners

Health Care Organizations

Financial Services Organizations

Controlled-Circulation Media

Quiet Enjoyment Infrastructure / Instigation #11

Public Roadways Infrastructure

Access to any server that is part of the DNS system or any significant router etc. should be by means of a credential that is signed by a Tabelio™ Birth Certificate.

Quiet Enjoyment Infrastructure / Instigation #12

Usable Vocabulary Infrastructure

What department of the typical enterprise insists upon autonomy?

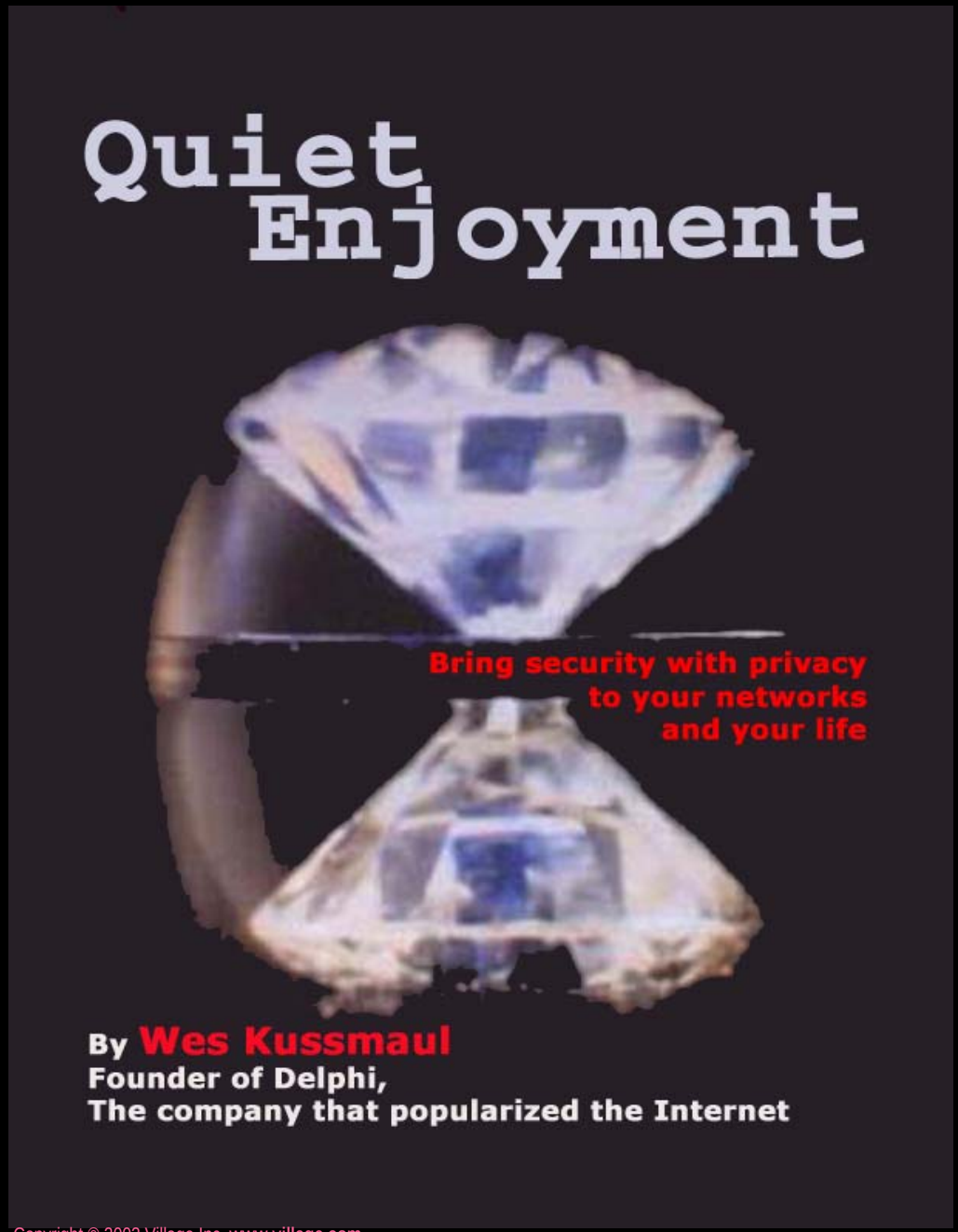
Why? How can that possibly work?

IT designs, builds and manages facilities. The CEO need not understand construction materials to know what facilities she needs.

The Usable Vocabulary Infrastructure provides he CEO with a linguistic means to manage IT as she must manage every department in order to be effective.

The Quiet Enjoyment Infrastructure

Identity is the Foundation of Security ™



Available at abyx.com and in bookstores early 2004