Digital Signature Legislation

Why use a hammer to pound a screw when you have a wrench?

— ji

Introduction

This is a cross-disciplinary field

- Few lawyers understand the technical issues
- Even fewer techies understand the legal issues
- Greenfields solutions designed by those who understand both tend to look nothing like the expected approach
  - AADS/X9.59
  - EDI/trading agreement-based approaches
  - IRS 1040 signing

Introduction (ctd)

It's a two-level problem

- Political/legal
- Technical

Not, it's really a four-level (2 × 2) problem

- Political/legal in theory (legislation)
- Legal in practice (case law and court decisions)
- Technology in theory
- Technology as it really works

Introduction (ctd)

Techies have no political authority and try to develop technical solutions to political/social problems

Politicians don't understand the technology and pass vague laws in the hope that the market will sort it out

It's a very hard problem to solve

- No consensus on how to do it

Typical approach

- Digital signature law is passed
- Published commentary on it is usually dissenting opinions

Why do we need Dig.Signature Legislation?

Existing commerce uses paper-and-ink signatures

We need e-commerce

→ We need Digital Signature legislation

A horse is a mode of transport

A car is a mode of transport

→ A car is a horse

Result: Laws requiring people to walk in front of cars waving red flags and firing pistols

- Signing a mortgage (paper) is very different from an online credit card purchase under MOTO rules (electronic)

What is a Signature?

A signature establishes validity of a document to allow the reader to act on it as a statement of the signer's intent, and leaves evidence to that effect afterwards

Signatures represent a physical manifestation of consent

- Can be enforced by a court if you later try to repudiate them
- A digital signature must provide a similar degree of security

A signature is *not* just authentication

- When you sign a document (e.g.cheque), you're making a promise, not authenticating yourself
- Even when you sign in to a building, you're engaging in ritual, not authenticating yourself

What is a Signature? (ctd)

Typical signature functions are

- Associate the signer with a document
- Prove involvement in the act of signing
- Provide proof of the signer's involvement with the content of the signed document
- Provide endorsement of authorship
- Provide endorsement of the contents of a document authored by someone else
- Prove that a person was at a given place at a given time
- Meet a statutory requirement that a document be signed to make it valid

What is a Signature? (ctd)

Some countries have requirements that contracts for the sale of goods above a certain value be "signed" to be enforceable. This signature can be

- A signature in the generally-accepted sense
- A stamp
- A typewritten signature
- Use of company letterhead

A signature then isn't necessarily a handwritten signature

- Stamp
- Chop-marks
  - Probably the closest real-world equivalent to digital signatures

What is Notarisation?

The term "notarisation" has a very specific legal meaning

- Nothing like the way it's used in relation to digital signatures

Requirements for notarisation (from the American Notarization Association)

- Face-to-face interaction with the notary
  - Allows the notary to identify the signer
  - Allows the notary to judge that the signer is willing and aware of their actions
- Identification through personal knowledge, witnesses, or documents

... continues...

What is Notarisation? (ctd)

... continued...

- Acknowledgement by the signer of their participation in the notarisation process
- Notary's observation that the signer is not under duress
- Notary's observation that the signer is aware of their actions

Digital signatures *cannot* fulfil these requirements

> Public Key Infrastructure (PKI) services do not provide the assurances associated with official notarial acts by a state-commissioned Notary Public and lack the legal authority of proper notarization, which is to provide prima facie evidence of the truth of the facts recited in the certificate and to establish the genuineness of the signatures attached to an instrument
>
> — "A Position on Misleading Usage of Notary Terms in the Electronic Age", American Notary Association

Real-world vs. Electronic Signatures

Real-world paper-and-ink signatures use

- A standard pen
- A standard hand/wrist
- Standard handwriting

But…

- The user is aware of the importance of their action
  - Writing a date on a document
  - Writing a signature on a document

Real-world vs. Electronic Signatures (ctd)

Different weight is given to the signature depending on context

- Inter-office memo
  - An "X" will do
- Credit card receipt
  - Check the amount
- Mortgage agreement
  - Get a lawyer to check it for you
  - Some banks require a letter from a lawyer indicating that they've checked the mortgage agreement on behalf of their client

Real-world vs. Electronic Signatures (ctd)

The difference between plain handwriting and a signature is informed consent

- One of the uses of signatures is to make parties aware of the consequences of their actions

This is why paper signatures are still explicitly required for

- Transfer of interests in land
- Especially solemn transactions (wills, affidavits)
- Consumer protection
  - Ensures that consumers get a paper record and/or are forced to stop and think

Real-world vs. Electronic Signatures (ctd)

Digital signatures need to artificially split key functionality because the standards are mostly written by technologists who can't define law or social policy

What type of key/security measures do you use for:

- Signing a challenge-response authentication token?
- Signing a letter of introduction?
- Signing an inter-office memo?
- Signing a purchase order?
- Signing a receipt?
- Signing a will?

Real-world vs.Electronic Signatures (ctd)

The credit-card approach

- You may use your VISA with approved VISA merchants under these conditions…
- You may use the XYZ signature key with approved XYZ business partners under these conditions…
  - Identrus adopt this approach
- Difficult to enforce on a typical Windows box where all keys are equal

Other approaches are still awaiting legal test cases

Real-world vs.Electronic Signatures (ctd)

Long-term electronic signatures are a problem

- 30% of all contracts are mortgages
- Valid for 20-30 years

Most certificates expire after 1 year

- X.509 has a mechanism for separating lifetime of signing key and verification key, but PKIX prohibits its uses
- Attempted workarounds through various complex, arcane, and mostly untested mechanisms like timestamping and secure archiving

Real-world vs.Electronic Signatures (ctd)

In practice, signed messages (intended to be seen by humans rather than automated processes) are very rare

- Users check authentication based on message contents (semantic integrity), not digital signatures

Example: S/MIME signatures

- S/MIME standards group debated using digital signatures on their mailing list
  - For people you know, you can authenticate messages based on content (semantic integrity)
  - For people you don't know, a signature is irrelevant
- Also, digital signatures are just a royal pain to work with
- Result: The S/MIME standards developers decided to forgo using S/MIME signed messages

Real-world Approximations to Dig.Sigs

Closest analogue to digital signatures is probably cheque cards

- Banks are liable for accepting forged cheques
- When merchants accept them, they have to take liability even though they don't have the verification facilities that banks have

Banks issued cheque cards to allow merchants to verify signatures (certificates)

- Cheque card blacklists were used to revoke them (CRLs)

General Requirements for Digital Signatures

The signing key must be controlled entirely by the signer for non-repudiation to function

The act of signing must be conscious

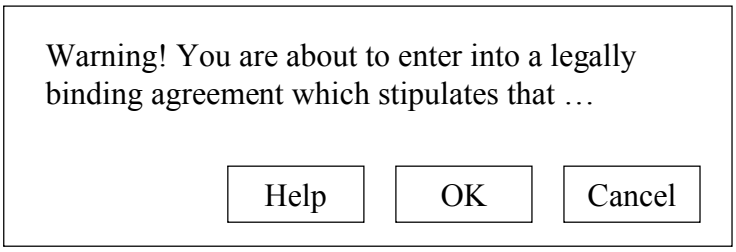
- The "Grandma clicks the wrong button and loses her house" problem
- "You are about to enter into a legally binding agreement which stipulates that ..."

Dialog boxes become legal documents

- Lawyers (not UI designers) need to design your user interface
- The case will be heard by a 60-year old judge with a fine arts degree

General Requirements for Digital Sigs (ctd)

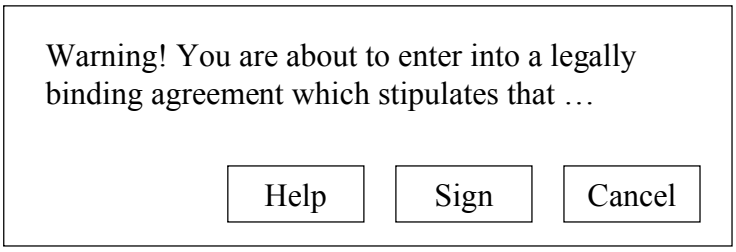
Signature dialog, first attempt



- "My client was acknowledging a warning, not creating a signature"

General Requirements for Digital Sigs (ctd)

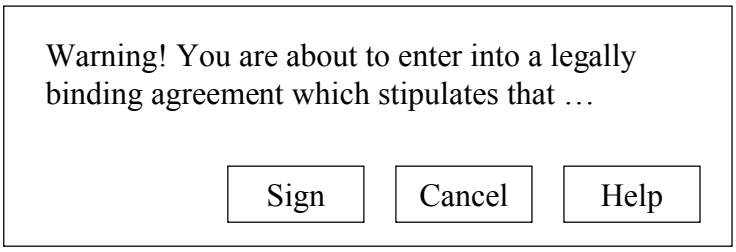
Signature dialog, second attempt



- "My client thought she was cancelling the action due to non-standard placement of buttons"
  - 'Sign' button is where the 'Cancel' button would normally be

General Requirements for Digital Sigs (ctd)

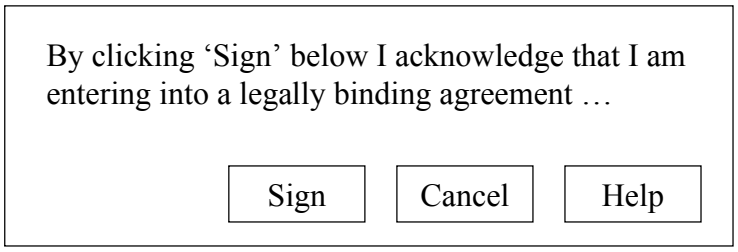
Signature dialog, third attempt



- This is still a warning phrased as "about to" rather than "are entering into"

General Requirements for Digital Sigs (ctd)

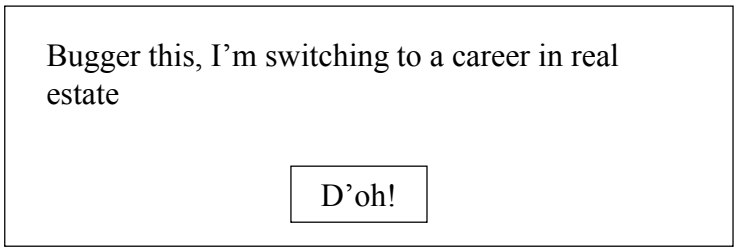
Signature dialog, fourth attempt



- Even this may still have holes

General Requirements for Digital Sigs (ctd)

Signature dialog, fifth attempt



- Programmer was informed that they needed to create a mechanism for preserving the dialog + user click as evidence

General Requirements for Digital Sigs (ctd)

May require a traditional written document to back up the use of electronic signatures

- "With the key identified by ... I agree to ... under the terms ..."
- Written German HBCI (Home Banking Computer Interface) agreement (Ini-Brief) has
  - Key owner identification information
  - Date/time
  - Key and hash of key
  - "I certify that this key is used for my electronic signature"

General Requirements for Digital Sigs (ctd)

Other electronic signature forms such as voice signatures are also a possibility

- Have the user read out a statement like "I, Joe Bloggs, hereby sign the funds transfer of ...., on 27 May 2007"
- Provides strong evidence for a court
  - This is an original statement of the signer's intent, not an entry in a database
- Clearly demonstrates intent, knowledge, and voluntary action by the user

Non-Repudiation

Most digital signature products claim they provide non-repudiation

- It sounds good, and doesn't cost anything to claim this

Technical non-repudiation is almost impossible to achieve

- Existence of a paper-and-ink signature implies that you were involved and saw (if not read) what you were signing
- Existence of a digital signature implies that at some point something, somewhere performed a mathematical operation on some data

Non-Repudiation (ctd)

Digital signatures can be almost trivially repudiated

- "The software didn't properly make me aware of the consequences of my actions"
  - "Grandma clicks the wrong button and loses her house"
- "A virus did it" (the universal excuse)
  - A nontechnical jury will be quite used to any glitch being the fault of "a virus"
- Publish your private key in the paper
  - Google for private key file types to see how common this is
  - Can be punished for carelessness, but not for the contents of signed messages
- If the message is timestamped, claim you didn't know at the time that your key was stolen

Non-Repudiation (ctd)

Non-repudiation can best be achieved through laws guaranteeing repudiation

- That's "guaranteeing *repudiation*", not "guaranteeing non-repudiation"
- c.f. Reg.E/Reg.Z for credit cards/ATM cards

Liability issues are the Achilles heel of digital signature laws

Reg.E/Reg.Z

Congress passed laws guaranteeing repudiation to force banks to provide appropriate consumer protection

- Report loss within 2 days: No liability
- Report loss within 2-60 days (time to get a bank statement): Liability of $50 (value of one average transaction at the time the law was passed)
- Note that physical loss is immediately evident to the card owner; electronic fraud isn't

Reg.E/Reg.Z (ctd)

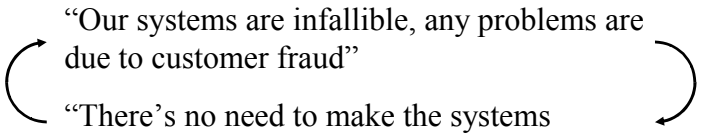
Other countries have similar legislation

- UK Consumer Credit Act with a liability limit of £50.
  - However, UK law has the nebulous loophole of "gross negligence" which allows banks to dump liability on the consumer
- Australian EFT Code of Conduct
  - Worked out by banks, consumers, and regulators after banks had dumped all liability on their customers

No current digital signature law is capable of providing Reg.E/Reg.Z consumer protection

Reg.E/Reg.Z (ctd)

"Impossible-to-forge" digital signatures allow all liability to be shifted onto users



This was a severe problem with UK banks in the 1980s and 1990s

- Some serious miscarriages of justice occurred because banks blamed any disputed transaction on customer fraud, and courts believed them
- 'Chip & PIN' is an attempt to return to the good/bad old days

Open vs. Closed Systems

In an open system

- Signer uses some form of universal ID from a third-party CA for signatures
  - Can use the same universal signature to buy a piece of clip art or a Picasso
- Parties have no previously established network of contracts to rely on
- No way to handle liability
  - Cannot internalise the costs of the inevitable fraud that will occur
- Example open systems
  - Public PKIs/CAs

Open vs. Closed Systems (ctd)

In a closed system

- Members sign up to the rules of the club
- Only members who will play by the rules and can carry the risk are admitted
- Members are contractually obliged to follow the rules, including obligations for signatures made with their private key
- Electronic agreements are bilateral or multilateral, and backed by paper-based ones
- Example closed systems
  - EDI
  - SWIFT
  - ACH

Liability

CA issues a certificate to Alice. Alice's key is stolen by a virus. Alice immediately revokes her cert. At the same time, Bob dispatches $10,000 based on a signed withdrawal note from Alice. Who is liable?

- Alice exercised due diligence in immediately revoking her certificate
- The CA is a third party not involved in the transaction
- Bob exercised due diligence in verifying the CA-certified key

Liability (ctd)

To resolve this

- Bob does away with the CA
- If Bob is a bank, it manages its own records and authorisation mechanisms
- If Bob is a merchant, he uses established mechanisms such as using a bank as guarantor of the transaction

This is a return to the model used in existing EDI transactions

- This is a business problem, not a technical problem, and not necessarily a legislative problem

Liability in Open vs. Closed Systems

In a closed system, liability is handled via bilateral/multilateral trading agreements

In an open system, parties have no previously established network of contracts covering private key use on which they can rely

- On what basis do you sue someone when they repudiate a signature?
- Have they published a legally binding promise to the world to stand behind that signature?
- Do they owe a duty of care, actionable in the case of negligence?

Liability in Open vs. Closed Systems (ctd)

Possible ways to proceed

- Claim a duty of care where negligence resulted in financial loss
  - Generally negligence claims for pure financial loss won't support this
- Claim that publishing the key was a negligent misstatement
  - Unlikely that this will work
- Go after the CA
  - CA won't suffer any loss if the keyholder is negligent, so they can't go after the keyholder
- Dump liability on the relying party
  - Completely defeats the point of a PKI

Liability in Open vs. Closed Systems (ctd)

Pseudo-closed systems ("Let 10,000 CAs bloom")

- Theory: A CA for every occasion, each following the closed model
- Practice: Even a single PKI is already hard enough to do, we don't need to multiply this difficulty by 10,000
- Better to use 10,000 application-specific solutions than to take a one-size-misfits-all one and then not apply it to -all anyway

Open models remain popular

- Rigid, hierarchical models are appealing to governments
- One-size-fits-all approach is appealing to legislators
- Legislating a PKI is appealing to techies
- Everyone's "we gotta do something" itch gets scratched

Why One-size-fits-all Model Doesn't Work

Case 1: Banking

- Strict security, accounting, two-person control
- Example: Buying a PIN printer cable
  - Two people drive to a row of computer stores
  - One person selects a random store
  - The other person selects a random cable from the store
  - They drive back to the bank with the cable on the seat between them

Why One-size-fits-all Model Doesn't Work (c

Case 2: Healthcare

- You can violate any security rule as long as you can justify it later by saving the patient
- Example: Medical practice
  - Anything that stops the doctors doing their job is an impediment that needs to be removed
  - Lowest level of security granularity that can be achieved is "everyone in the practice"
  - First person in in the morning logs on
  - Everyone else uses their key for the rest of the day
  - Nurses/administrators know the doctor's keys, and are expected to use them
  - Saving the patient is more important than security

The Existing EDI Approach

Electronic Data Interchange

- X.12 in US/Canada
- EDIFACT in Europe
- Specialised variations, e.g. HL7 for medical EDI
- XML = EDI with the second-system effect
  - PL/I = Cobol with the second-system effect

EDI is the Cobol of e-commerce

- Boring and tedious
- 90% of everything depends on it

The Existing EDI Approach (ctd)

EDI is the archetypal closed system

Governed by interchange agreements

- Describe the rules that govern the business transactions
- Cover the responsibilities of each party
- Specify identification/authentication requirements
- Specify archiving requirements
- List technical and legal responsibilities of parties, including banks
- Application-specific, custom digital signature laws

Security traditionally provided by passwords or MACs

The Existing EDI Approach (ctd)

The EDI process is handled via standard business mechanisms

- (US) Business Records Exception allows standard business records to be treated as evidence (rather than hearsay) in court
- Well-established mechanisms (and much legal precedent) for this
- It's much easier to manage a cheap trusted message store/audit mechanism than to solve a global infrastructure and policy problem
  - You need this information anyway for the auditors

Trust

This term appears constantly in relation to certificates

"Alice sees the certificate and trusts Bob"

What is trust anyway?

Types of trust

- Blind trust
  - Sometimes the only option, e.g. emergencies
  - "Is there a doctor in the house?"
- Swift trust
  - Based on a series of hedges to reduce potential loss
  - Trading with a new business

Trust (ctd)

- Deference-based trust
  - Disincentive to betray trust
  - Contract / auditing / "our systems are infallible, don't even think about it"
  - Regulated markets, e.g. banks
- Knowledge-based / historical trust
  - Based on established history / trading relationship
  - "We've been doing business with them for 10 years"
- Social trust
  - Based on emotions rather than rational thought
  - Little old ladies

Trust (ctd)

- Identification-based trust
  - Parties have common goals
  - "He's wearing the same uniform as me, we're on the same side"
- Indirect trust
  - Sometimes, trust can't be established directly
  - Establish indirect trust using third parties
  - Use a bank as guarantor

One type of trust can bootstrap another

- Swift → knowledge-based

Trust Taxonomy

Type of Trust	Mechanism
Blind	None necessary
Swift	None necessary
Deference-based	Bilateral trading agreements
	Contracts/legal agreements
	Laws
Knowledge-based / historical	None necessary
Social trust	—
Identity-based	Identity certificates

Types of Trust

Trust can be grouped into one of three classes

- Mechanistic trust
  - Based on positive evidence
  - "We've done it before and it worked"
- Religious trust
  - Based on faith
  - No evidence, but we hope for a positive outcome
- Psychotic trust
  - Based on negative evidence
  - "We've done it before and it didn't work"

Much current PKI "trust" is either religious or psychotic

Things that Affect Trust

Trust is affected by

- Culture
- Third-party ratings
  - Better Business Bureau
  - Consumer Reports
  - Not always reliable: TRUSTe handles violations by changing its policy so that they're no longer violations
- Second-party opinions
  - "My brother bought one, he's had nothing but trouble with it"
- First party information
  - "We will not sell your private data to third parties"
    - (We will, however, trade it to them without actually selling it)

Things that Affect Trust (ctd)

Trust has value

- Business goodwill
  - Trust → money
- Reputation capital
  - Use money to buy "trust"
  - Money → trust

Trust degradation

- Without reinforcement, trust decays over time
- Trust may be deliberately destroyed
  - "My credit card has been stolen"
  - Prevents parties from making decisions based on invalid trust data

Trust (ctd)

You can't create trust with cryptography, no matter how much cryptography you use

You can't create trust with legislation, no matter how much legislation you use

Digital Signature Legislation

Prescriptive approach

- You must do exactly this to comply
- The government can stimulate business growth by resolving uncertainty
- Driven by techies
- Creates business models that would never evolve naturally in the marketplace

Digital Signature Legislation (ctd)

Hands-off approach

- Anything reasonable is fine
- The government can stimulate business growth by removing barriers and letting the market decide
- Driven by lawyers
- Doesn’t enforce any business models since it doesn’t really enforce anything

Prescriptive Approach

Utah Digital Signature Act

German Digital Signature Law

Italian Digital Signature Law

- Later laws worked around the problems turned up by earlier ones

ETSI Digital Signature Draft

Swedish Electronic ID card (SEIS)

Hands-off Approach

California Digital Signature Law

Massachusetts Electronic Records and Signatures Bill

US E-Sign Act

Singapore Electronic Transactions Act

UNICTRAL Model Law on Electronic Commerce

- Almost everyone is now basing their laws on this

Other Approaches

Mixed Approach

- EU Directive on Electronic Signatures

"It's already handled" approach

- UK Law Commission
- Australian E-commerce Experts Group

Politics (and Money)

Local or domain-specific laws can override a national signature law, despite what the national signature law may say

Example: Australian real estate transactions

- Have very distinctive requirements for signatures
- Individual states (not the Commonwealth) have jurisdiction
- Land tax is the No.1 revenue earner for states
- States will *never* give this up

Utah Digital Signature Act

The first digital signature act, passed in 1995

The Law of X.509

- Requires public-key encryption based signatures, licensed CAs, CRLs, etc etc

Duly authorised digital signatures may be used to meet statutory requirements for written signatures

Liability of CAs is limited, signers and relying parties assume the risk

Utah Digital Signature Act (ctd)

Signature carries the evidentiary weight of a notarised document

- If your key is compromised, you're in serious trouble
  - The Windows virus du jour can give a third party the ability to issue notarised documents in your name
- If you hand over your key to a third party, you're in serious trouble
- If a signature is verified, it's assumed that the user has accepted the certificate and signed the message
  - In order to challenge this, the user must prove a negative
  - c.f. proving "Aliens exist" vs. "Aliens don't exist"

Utah Digital Signature Act (ctd)

Drafters of the act assumed that the spectre of liability would prevent the emergence of commercial CAs

- CA would be required to take exceptional, costly steps to confirm identity, and yet still issue an erroneous cert
- Every party that relied on this could claim against the CA
- CA's liability would be staggering

CAs could avoid this by entering into contracts with certificate holders

- Wouldn't work for relying parties, who are the ones likely to incur losses

Utah Digital Signature Act (ctd)

Solutions

- Use a closed system (again)
- Dump liability on the cert holder

Users carry (potentially) infinite liability

> No rational consumer would accept this level of risk in a marketplace transaction
>
> — Vice-chair of ABA Electronic Commerce subcommittee

- Little-used because of this

Nevertheless, it didn't stop other countries from copying it

> When a digital document […] bears the sender's digital signature it shall be presumed […] originated by the sender
>
> — Argentinian *Ley De Firma Digital* Nº.25.506

German Digital Signature Law

Like the Utah act, based on public-key technology

Requirements

- Licensed CAs that meet certain requirements
  - CAs must provide a phone hotline for revocation
- Identification is based on the German ID card
  - This type of identification isn't possible in most countries
  - Allows pseudonyms in certificates
- Key and storage media must be controlled only by the key owner
  - Key may be generated for the user by the CA if strict controls are followed to ensure that no copies are retained
- Provisions for timestamping and countersigning

German Digital Signature Law (ctd)

Signatures from other EU countries are recognised provided an equivalent level of security is employed

Multilevel law

- Signaturgesetz (SigG) provides general framework
  - Defines a digital signature
  - Defines the role of a CA
  - Defines certificates and outlines how they're handled
- Signaturverordnung (SigV)
  - Sets out operational details and responsibilities of a CA
- Signatur-Interoperabilitätspezifikation (SigI)
  - Technical specification to implement the SigG and SigV
  - Specifies data formats, algorithms, timestamping and directory service mechanisms, etc etc

German Digital Signature Law (ctd)

Example

- SigG: A private key must be protected
- SigV: A private key must be protected in the following circumstances using certain technical measures
- SigI: Here are the technical measures

While compliance with the law has been described as 'voluntary', it is difficult to see how alternatives could operate

— Report of the Australian Electronic Commerce Experts Group

German Digital Signature Law (ctd)

Details are set out in the implementation guidelines

- Extremely detailed (over 300 pages)
- Specifies things like
  - Hash and signature algorithms
  - Random number generation for keys
  - Personnel security
  - Directory and timestamping services
- Spawned hundreds of pages of supplementary documentation covering further digital signature issues
  - BSI publishes a CDROM full of these things
- Criticised as being too detailed and complex to follow
- Later watered down to try and make it more workable

German Digital Signature Law (ctd)

Case study: Telesec CA (Deutsche Telekom)

- SigG/SigV-compliant CA
- $12M to set up
- 25 full-time staff
- 250 certificates issued
  - ~$50,000 per certificate

Case study: TrustCenter CA (Commerzbank, Deutsche Bank, Dresdner Bank, Hypo Vereinsbank)

- Banks withdrew their support in early 2004
- Declared insolvent in September 2005

Of the original 15 providers, 13 have now gone bankrupt

Italian Digital Signature Law

Similar to the German law, but all requirements are listed in one place

Everything has to be certified to various ITSEC (later Common Criteria) levels

- Key generation devices must be certified to ITSEC E3 with a HIGH level of robustness
  - In practice, this forces everyone to use smart cards for key management
- The OS must be ITSEC F-C2/E2 or TCSEC C2
- Access to the system must be controlled, users identified, usage logged
- CAs must be ISO 9000 certified
- This severely limits the technology that can be used

Italian Digital Signature Law (ctd)

Signature mechanism must present the data to be signed in a clear and unambiguous manner, and ask for confirmation of the signature generation

- Allows for automated signature generation provided that this is "clearly connected to the will of the subscriber"

Certificates must contain users name, date of birth, and company name

- Allows pseudonyms, but this must be indicated in the cert and the CA must record the real identity

Italian Digital Signature Law (ctd)

Includes some bizarre requirements that are at odds with the way the rest of the world does things

- All prescriptive laws end up with these at some point
- Makes use of COTS software impossible
  - Half the CAs in Europe seem to rely on this as their business model

Italian Digital Signature Law (ctd)

CA must

- Verify that the key hasn't been certified by another CA
  - Another prove-a-negative requirement
- Verify that the user possesses the private key
- Publish certificates in LDAP directories
- Publish details on themselves (company name, address, contact details, terms and conditions, substitute CA)

The fixation with (expensive and complicated) certification had made deployment problematic

Italian Digital Signature Law (ctd)

System failed because of problems with certification and with vendors' ability to deliver

- Preferred vendor couldn't deliver evaluated CA hardware
  - Users spent millions on hardware that (eventually) wouldn't meet the requirements
  - Lawsuits between users, vendors, government departments

Users faked it with software-only solutions

- Run a PC in a locked back room

ETSI Digital Signature Draft

ETSI TR/TS 101 0*xx* reports specify technical requirements for signatures

- Role of signer (e.g. Financial director) is more important than the name
- Signature must be dated to allow later dispute resolution

References various standards efforts (e.g. PKIX) for further study

Privilege attribute certificates (PACs)

- Defined by ECMA, special short-lived (1 day max) certificates
- Vouch for a certain property of the user

Swedish Electronic ID card (SEIS)

Smart-card contains three keys

- Authentication (= X.509 “digital signature”)
  - Card supports a challenge-response protocol for authentication
  - Card signs a random challenge from the remote system
- Digital signature (=X.509 “nonrepudiation”)
- Encryption

The 3-key design was based on careful technical and legal analysis of digital signature requirements

Swedish Electronic ID card (SEIS)

This approach was later abandoned because Windows can't handle two types of signing keys

- "Digital signature legislation, say hello to the real world"
- "Legally sound" or "Works with Windows": Pick one
- Windows often ignores key usage
  - Encryption key can sign
  - Signature key can encrypt
  - Convenient: Allows users to use the same key for everything

SEIS (ctd)

Card doubles as a standard ID card (photo, signature, etc)

Cards are issued by

- Government agencies
- Financial institutions
- Companies to their employees

Usage is governed by the SEIS Certification Policy

- Backdoor digital signature law
- Covers the certificate issuing process, security auditing, physical and procedural security, key management and protection

SEIS (ctd)

- Key may be generated by the CA for the user provided that strict controls are followed
  - Two-person security
  - No copy of the key is retained by the CA
  - PIN-protected device is physically handed to the user by the CA
    - User signs a document acknowledging receipt
  - Activation PIN is delivered over a separate channel
    - User is told to immediately change the PIN
- Complex physical and procedural security procedures for cards

California Digital Signature Law

Very broad, allows any agreed-upon mark to be used as a digital signature

- Western culture has no real analogue for this
- Asia has chop-marks, a general-purpose mark used to authenticate and authorise

One-sentence digital signature law: "You can't refuse a signature just because it's digital"

- Many later laws followed this model

Strongly influenced by the Utah Act

- "Anything but that"

Massachusetts Electronic Records and Signatures Bill

A signature may not be denied legal effect, validity, or enforceability because it is in the form of an electronic signature. If a rule of law requires a signature [...] an electronic signature satisfies that rule of law

A contract between business entities shall not be unenforceable, nor inadmissible in evidence, on the sole ground that the contract is evidenced by an electronic record or that it has been signed by an electronic signature

The Massachusetts law doesn't legislate forms of signatures or the use of CAs, or allocate liability

- "Attorney's Full Employment Act of 1997"

US E-Sign Act

Electronic Signatures in Global and National Commerce Act

> This bill literally supplies the pavement for the e-commerce lane of the information superhighway
>
> — Senator Spencer Abraham

Act was signed on paper and electronically

- Bill Clinton revealed his password ("Buddy") after the signing, rendering the electronic signature contestable (lack of diligence)

US E-Sign Act (ctd)

Massachusetts signature law taken to extremes

- Signatures can be a "sound, symbol, or process attached to or logically associated with a contract or other record"
  - "Press 9 to sign a binding contract, or 1 to hear this message again"
  - "Click here to enter into a legally binding agreement"
- Online comparison shopping may cause problems because not buying is a "withdrawal of consent"
  - Enforceability will probably take a court case to decide
- Vendors may charge extra for physical items (disk media, manuals, but also printed invoices)
  - Consumers are charged extra if they want a valid audit trail

US E-Sign Act (ctd)

Some records *cannot* be delivered electronically

- Court orders
- Wills
- Cancellation/eviction/foreclosure notices
- Health/safety warnings/notices

Pre-empts state legislation which is more strict than the E-Sign Act

US E-Sign Act (ctd)

Law is about *electronic* (rather than digital) signatures

- Journalists who contacted the House discovered that the people involved in creating the Bill weren't aware that there was a difference
  - They were too busy mangling metaphors to notice
- Bill was prepared with input from Dell, Gateway, Hewlett-Packard, Microsoft, and other vendors
  - No consumer advocacy groups were consulted
- The finished Act appears to be a means of imposing UETA (Uniform Electronic Transactions Act, sibling of UCITA, opposed by the attorney-generals of most states) by stealth
  - Would help make things like (currently dubious) click-through and shrink-wrap licenses legally binding

Singapore Electronic Transactions Act

Follows the one-sentence signature law model

- Where the law requires a paper signature, an electronic one will do

Offer of acceptance of contracts may be expressed electronically

Signature apparatus must be under sole control of signer

Singapore Electronic Transactions Act (ctd)

Certificate requirements

- Cannot publish a certificate known to be false
- Certificates must specify a reliance limit
  - Optional feature of other laws, e.g. German law
  - Of dubious value (just re-use the cert many times)
  - Static solutions to dynamic problems don't work

Compliant CAs are not liable for certificate problems

UNCITRAL Model Law on Electronic Commerce

UN Commission on International Trade (UNCITRAL) model e-commerce law

Countries felt that existing legislation didn't contemplate the use of e-commerce, and needed updating

- Existing legislation implies limits by prescribing the use of "written" or "signed" documents
- Model Law defines a functional equivalent approach for electronic documents/signatures
  - Ensures that electronic signatures can provide the functions required of paper documents

Twelve years in the making

UNCITRAL Model Law on E-Commerce (ct)

Information shall not be denied legal effect, validity, or enforceability solely on the grounds that it is in the form of a data message

Where the law requires information to be in writing, that requirement is met by a data message…

Where the law requires a signature of a person, that requirement is met in relation to a data message…

- The signature method indicates a person's approval of the message contents
- Signature method is as reliable as appropriate

UNCITRAL Model Law on E-Commerce (ct)

Almost everyone is passing laws based on this model law

- It's trendy
- All the other kids are doing it
- "We've passed this new law and lo! Our e-commerce functions no worse than before"
- Still an "Attorney's Full Employment Act"

UN Draft Articles on Electronic Signatures

Follows the one-sentence signature law model

- Includes a rationale for each point

Defines two levels of signature

- "Electronic Signature" = data attached to a message to indicate a signers approval of the message
- "Enhanced Electronic Signature" = electronic signature with extra constraints
  - Unique to the signature holder
  - Verifiable through a standard procedure
  - Under the sole control of the signer

Extremely broad and technology-independent

Specifies (rather vague) reliance and obligation details

UNCITRAL Model Law on Electronic Signatures

UN Commission on International Trade (UNCITRAL) model digital signature law

Refines the UNCITRAL E-commerce Law ("You can't refuse a signature just because it's digital") and Draft Articles

- Five years in the making
- Eventually drifted towards a focus on PKI
- Uses standard terms ("signature", "certificate") in novel ways to make them non-specific
- Worded so as to still allow mechanisms like "click-OK" for electronic signatures
  - Should not discourage "any method of electronic signature"

UNCITRAL Model Law on E-Signatures (ct)

Requires conditions for all signatures similar to the UN Draft Articles for Enhanced Electronic Signatures

- Appears to make CAs optional, but they're more or less assumed to be present

Recognises certificates from other countries issued under equivalent terms

- Pushes some regulatory issues back to the Model E-Commerce Law

Includes a rationale for all points

Makes comments about liability of all parties but "does not specify either the consequences or the limits of liability"

EU Directive on Electronic Signatures

Defines an electronic signature as linking signer and data, created by a means solely controlled by the signer (not necessarily a cryptographic signature)

Precedes the directive itself with the intended aims of the directive

Makes accreditation and licensing voluntary and non-discriminatory

- No-one can be prevented from being a CA
- Intent is to encourage best practices while letting the market decide
- Was rendered ineffective by countries tying participation in government programmes to accreditation

EU Directive on Electronic Signatures (ctd)

Electronic signature products must be made freely available within the EU

Electronic signatures can't be denied recognition just because they're electronic

Absolves CAs of certain types of liability

- Provides for reliance limits in certificates

Recognises certificates from non-EU states issued under equivalent terms

Allows for pseudonyms in certificates

EU Directive on Electronic Signatures (ctd)

Recognises that a regulatory framework isn't needed for signatures used in closed systems

- Trust is handled via existing commercial relationships
- Parties may agree among themselves on terms and conditions for electronic signatures
- Keys may be identified by a key fingerprint on a business card or in a letterhead

Much cross-pollination with UN Draft Articles/Model Signature Law, but with enough differences to make them incompatible

- UN later dropped the two-level Signature/Enhanced Signature distinction

EU Directive on Electronic Signatures (ctd)

Makes use of Advanced Electronic Signatures, which are tied to individuals

Question: What about large corporations, who would need to hire hundreds of people to personally sign e-invoices, etc?

Answer #1: Use EDI, which sidesteps the use of e-signatures

Answer #2: Fake it with Qualified Certificates issued to a pseudonym for a company (see next slides)

EU Directive on Electronic Signatures (ctd)

Specifies Qualified Signatures, which take Advanced Signatures a step further

- Must be treated in the same way as a handwritten signature
- Doesn't however regulate its legal use and consequences
- Tied to an individual signer, exclusively under their control

Based on a Qualified Certificate, with accompanying Qualified CA

- Strict controls over certificate issuance to individuals

EU Directive on Electronic Signatures (ctd)

In practice, qualified certificates are issued to companies by fudging the issuing process

- Issue the certificate to an alias for a company
  - Use the ability for a QC to contain a pseudonym
- Does a complete end-run around the QC legal requirements

Uncertainty as to what demand is actually being met by Qualified Certificates (apart from their utility to those doing the certifying)

> There is currently no natural market demand for Qualified Certificates and related services […] very few applications are in use today and they are almost completely limited to e-government
>
> — Stefan Kelm, e-Signature Law Journal

EU Directive on Electronic Signatures (ctd)

Case study: S-Trust (German banks' CA)

- €68 for the certificate (loaded into German Geldkarte cards), €43 for the card reader, €26 for the software (~USD190 total)…

  … assuming you can actually find the required product

  - Only two of ten listed S-Trust partners actually carried the product

  > The [QC-based banking] demonstration provided no indication of what advantages it held over conventional online banking. Speed certainly wasn't one of the improvements
  >
  > — iX, German computer magazine reviewing the use of QCs for online banking

UK Law Commission

UK Law Commission concluded that no special legislation is necessary

- Email and web sites are already in writing within the usual statutory meaning
- Typed names or "click-OK" count as signatures
- Use of public-key encryption affects the weight of the evidence in court, nothing more

Follows the analogy of technology like microfiche

- What's on the fiche is writing even if you need a machine to interpret it

UK Law Commission (ctd)

The law has historically been very accommodating of new commercial methods

- Use of stamps, company letterhead as "signatures"

In general, legislation isn't needed

Australian E-commerce Experts Group

Recognised that the law typically requires "best available evidence"

- Original document if possible
- Alternatives are acceptable (e.g. a fax if the original is unavailable)

More progressive laws already explicitly allow electronic evidence or "in any form"

- Something from which a document can be recreated by some means

Some cases specifically require originals to guarantee uniqueness or provide the earliest record in time

Australian E-commerce Experts Group (ctd)

> The law already recognises contracts formed using facsimile, telex […] unlikely that recognition would not be accorded to contracts formed […] electronically. The principles are the same in the case of both paper and electronic communications
>
> — Report of the Australian Electronic Commerce Experts Group

- Some precedent in existing law for contracts entered into by computers
  - Social Security Act treats computer decisions on allowances as made by humans

The Digital Signature Litmus Test

The legal test: Can your law/mechanism provide Reg.E/Reg.Z-type protection for consumers?

- If the answer is "No", it's just handwaving

The practical test: Is your system implementable with everyday technology and moderate effort?

- If the answer is "No", it'll never fly

The NIMBY test: Would you want to be the test case?

- If the answer is "No", why would you expect others to use it?

Conclusion

Open systems don't work

- No way to handle liability (fail the legal test)

Prescriptive approaches don't work

- Excessively complex and costly, still don't fix the liability problem (fail the practical and legal tests)
  - SigG: 10 years of signature law, no appreciable results

Hands-off approaches don't work

- Don't really solve anything (fail the legal and NIMBY tests)

What's left

- Closed systems
- Use existing law/mechanisms/precedent