MAKING DIGITAL DATA TRUSTWORTHY IN THE CLOUD

Cian Kinsella – CEO, Digiprove

cian.kinsella@digiprove.com

Malaga 7th June 2013

My Background

- Been developing software since 1972
- Commercial and Freelance
- Co-founder of 3 Software Product Companies
- Have had many different responsibilities
- Still developing software, though…

- Digiprove's technology adds Trust to Digital data

What is the core issue?

- To be able to provide absolute proof of the integrity, authenticity and provenance of digital content when required. (detect any tamper).

- The Cloud adds further uncertainty:
  - Who has access to your data & communications?
  - How many times is it replicated?
  - Where is your data (and copies thereof)?
  - Who has access to your data

- You are placing Trust in an organisation, i.e. people, not technology

When is Trust Critical?

- Digital evidence
- In Court
- For Regulator/Compliance
- For Business decisions
- eDiscovery
- IPR/Copyright
- Retention compliance
- Digital Signing
- Cloud Data and Apps
- Social Media
- Financial Records

Proliferation of Digital Data

- Vast majority of content originates digitally:
  - Application software
  - Email
  - Microsoft Word
  - Digital cameras
  - Pro-tools Sound Production software
  - Final Cut Video Production software
  - Phones/Tablets: VOIP / Messaging (BYOD)

- Most of the rest ends up in digital domain
  - Scanned papers and images
  - OCR
- Usually no way to trace provenance

Characteristics of Digital Data

- It is intended by design to be manipulated
- It can be changed:
  - Text files
  - Microsoft Word and other documents
  - Email archives
  - PDFs
  - Sound recordings
  - Images
  - Database records & Logs
- It is communicated
- It can move location or be replicated

Questions to Consider

- Criticality of Data Integrity
  - What is consequence of integrity failure
- Who needs to trust it?
  - Internal – *basis for operational decisions*
  - Non-exec Directors / Boards – *basis for strategic decisions*
  - Auditors or Regulators – *basis for compliance*
  - External Stakeholders – *basis for trust & confidence*
  - Public/Citizen – *basis for trust and commitment*
  - Journalists – *for attributable quotes*
  - Courts – *evidence*

How trustworthy does it need to be?

- Depends on:
  - Criticality of business
  - Criticality of data

I trust our access controls:

Completely | Up to a point | Not Sure

Motivation to tamper or hack:

Little or none | Certain parties | Strong interest

Potential Consequences of undetected tamper:

Negligible | Unknown | Potentially Serious

Can some of the data become evidence?:

Very unlikely | Possibly | Probably


Criticality of Data
HR records
Financial Logs
Decision Support
Personal data
Tweets etc.
Action Logs
Financial data
Communications
Compliance
Records
Web-site
Standard Docs
User Manuals
Staff
Suppliers
Clients
Auditors/Regulators
Public
Courts
Potential Audience

Low Trust Examples

- Regulators
  - Often insist on "wet" signatures
  - Submissions must be in paper or fax
  - Retention of Original paper records
- Legal documents, contracts etc.
- Certificates, Diplomas
- E-Discovery Law
  - Spoliation allegations
  - Preservation Obligations
- Cloud generally

Low Trust should create demand for Digital Data Trust Solutions

Misplaced Trust

- Documents
  - PDFs
  - Scanned Images
- HTTPS web-pages
- (Some) Financial Audit Trails
- Cloud data
- Tweets and other social media

Misplaced Trust Example

PAYMENT

▸ **CREDIT CARD** **Please, charge in my credit card the total amount:** _____ €
(Registration + Accommodation)

□ VISA □ MASTERCARD □ AMERICAN EXPRESS □ OTHERS

Credit card number: Expiration date (month/year):

Credit card holder: Signature:

ACCOMMODATION and REGISTRATION FORM

IFIPTM'2013

June 3-5, 2013, Malaga, Spain

VIAJES El Corte Inglés

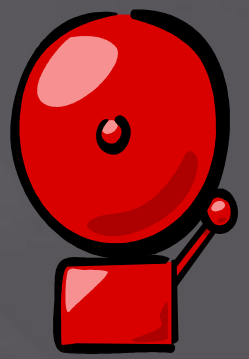
SEND **BY FAX** TO: *VIAJES EL CORTE INGLÉS* **Fax. +34 952 60 90 60 Phone: +34 952 062 654**

or **SCANNED BY E-MAIL** TO: malagacongresos@viajeseci.es

Requirements of a Data Trust Solution

- Have certainty that any content has not changed
  - Since creation date
  - Since authorised amendment
    (must include version history)

- Automatically detect if content changed outside permitted channels
  - Threat detection
  - Early alarm for attempted fraud
  - Early alarm for data corruption



Give visible assurance

Raise Alarm

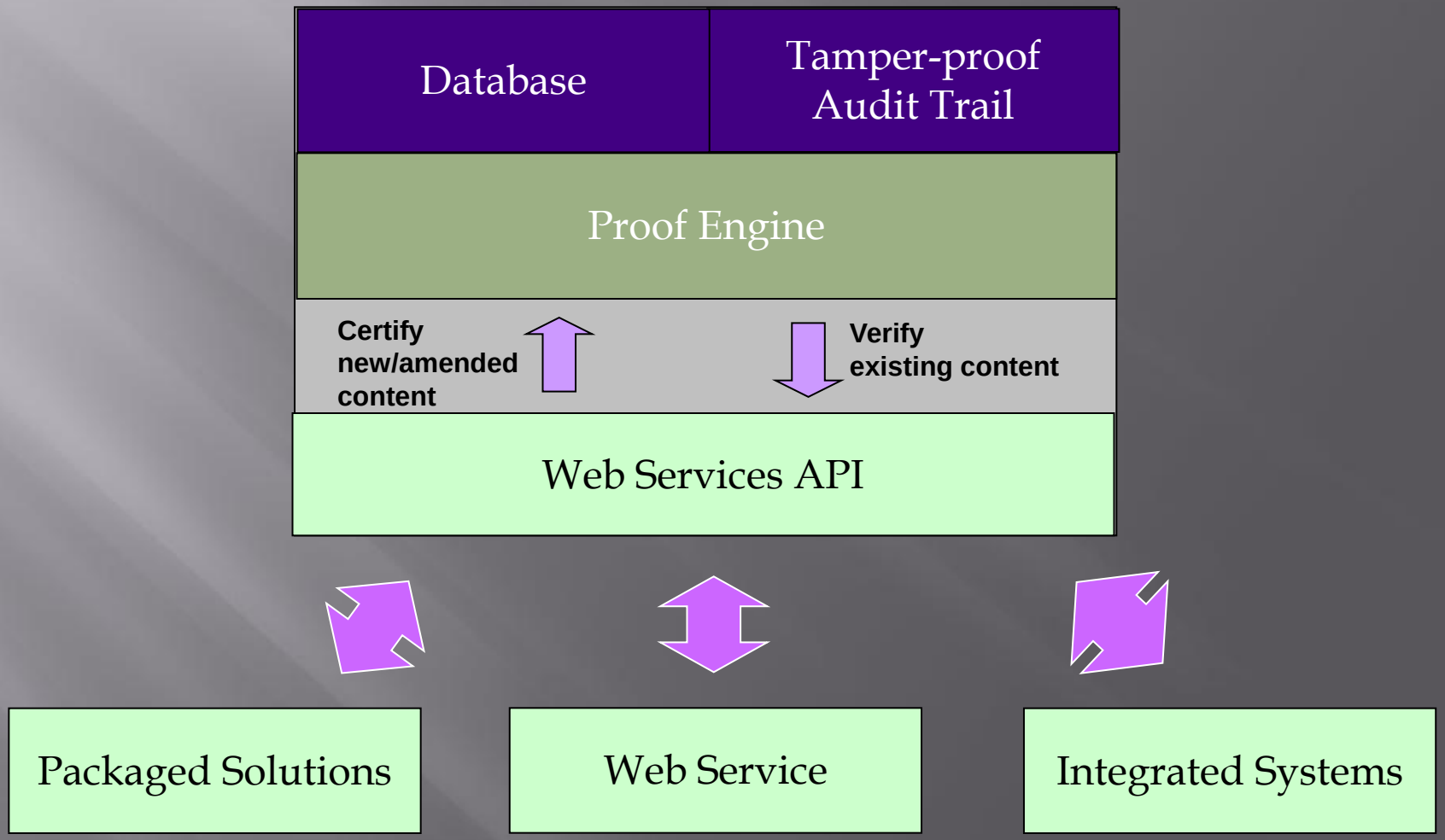
Requirements of a Data Trust Solution

- Establish Provenance
  - Who created?
  - Who witnessed?
  - Is signed / contains signatures?
  - Version History
- Other Metadata:
  - Data Type
  - Functional / How created (email, MS Word, camera etc.)
  - Where created – Location
  - Identity (like fingerprint)

Methods for Establishing Data Trust

	Description	Advantages	Disadvantages
Digital Signatures	Individual signs content - Binds content to individual and any change in content is detectable.	- Very Secure - Independent proof of identity - Can be extended with independent timestamp	- Dependent on "web of trust", independent certification of identities - Computationally expensive
Digital Fingerprinting	Use one-way "hash" algorithm to create unique fingerprint of each file/blob	- Easy to implement - Computationally light - Reliable at detecting file corruptions	- No intrinsic security - No intrinsic time-stamp - No key - No provenance - Certain algorithms have flaws (e.g. SHA1, MD5)
Checksum	Simple algorithm to identify content	- Very Quick - Reasonably	- As for digital fingerprinting

Overview


Database
Tamper-proof Audit Trail
Proof Engine
Certify new/amended content
Verify existing content
Web Services API
Packaged Solutions
Web Service
Integrated Systems

The solution is holistic:

STEP:	Function	Notes / Options
Digital Fingerprinting	Creates unique id/recognition key for each	Uses strong algorithm (e.g. SHA256)
Secure Fingerp		
Create timestar		e incorporates timestamp
Certify metadata	Establishes provenance	- User name, content abstract, version, GPS co-ordinates
Create transpa tamper-evider trail		chain of cally
Independent		b service
Automatic Verification	Gives visible assurance Detect / Alert tampers or corruptions	- On request - Periodic - Whenever content is accessed

Result: Creates proof of content & time-stamp and provides independent certification of this

It is impossible (even for Cert. Service Provider) to issue a back-dated certificate. Process does not rely on trust in any person or organisation.

Some Uses of this Technology

- Tamper-evident audit trails (regulated industries)
- Establish provenance & timestamp of legal documents
- Verify integrity of web pages as they are served
- Handwritten signatures on digital documents
- Meet e-Commerce legal requirements on retaining digital data
- Tamper-evident email archives
- Ediscovery lock-down

Applying to the Cloud

- Requires cloud & ground deployment of technology
- Multiple Points of certification:
  - For content created locally, evidenciate before upload
  - For content created in Cloud, evidencentiate immediately
  - For externally-sourced content, evidentiate immediately
- On Content presentation, verify locally

We are Interested in

- Ideas about Drivers for Recognition of Problem
- Raising our Profile
- Improving Our Core Offering
- New Deployments of our technology/service
- Academic Opinion and Input
- Other Forms of Collaboration

Thanks

cian.kinsella@digiprove.com