Cryptographer
Security Architect

Physicist
Transport Architecture

<table>
<thead>
<tr>
<th>Year</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>1998</td>
<td>PKI</td>
</tr>
<tr>
<td></td>
<td>elliptic curves</td>
</tr>
<tr>
<td></td>
<td>satellite PSN</td>
</tr>
<tr>
<td>1999</td>
<td>π-calculus VM</td>
</tr>
<tr>
<td>2000</td>
<td>control networks</td>
</tr>
<tr>
<td>2001</td>
<td>mobile identity</td>
</tr>
<tr>
<td></td>
<td>secure documents</td>
</tr>
<tr>
<td>2003</td>
<td>ENUM</td>
</tr>
<tr>
<td>2006</td>
<td>dotTel</td>
</tr>
<tr>
<td></td>
<td>hybrid encryption</td>
</tr>
<tr>
<td>2007</td>
<td>encrypted DNS</td>
</tr>
<tr>
<td>2010</td>
<td>concurrent VM</td>
</tr>
<tr>
<td>2011</td>
<td>national eID</td>
</tr>
<tr>
<td>2012</td>
<td>encrypted SQL</td>
</tr>
<tr>
<td></td>
<td>privacy by design</td>
</tr>
<tr>
<td>2014</td>
<td>uPass</td>
</tr>
<tr>
<td>2018</td>
<td>Redbush</td>
</tr>
<tr>
<td></td>
<td>Agora</td>
</tr>
</tbody>
</table>
The EU GDPR will increase privacy for individuals and give regulatory authorities greater powers to take action against businesses that breach the new laws. Here's what it means for your business:

**Tough penalties:** fines of up to 4% of annual global revenue or €20 million, whichever is greater. The regulation also applies to non-EU companies that process personal data of individuals in the EU.

**PRIVACY AND SECURITY**

- digital data is easily duplicated
- when data moves or is stored it generates metadata which is itself digital data
- processing data or metadata can reveal identity even if any personally identifying data it contains is encrypted
- so a system which respects privacy needs to know as little as practical about
- the data it processes
- the metadata it produces
UK LEGAL IDENTITY

➤ birth certificate and gender recognition certificate are the primary identity documents

➤ with either it's possible to get
➤ national insurance number
➤ NHS medical card
➤ passport

➤ name can be changed with a deed poll or a statutory declaration

➤ none of these documents include biometrics
ATTRIBUTES

➤ attributes are discrete facts
➤ dark hair
➤ wears black
➤ professional cryptographer
➤ fragments of an identity
➤ they may be entirely absent
➤ or some may be imprecise
➤ even a complete set may not be unique
➤ they're only as trustworthy as their origins
anonymity

pseudonymity
anonymity

pseudonymity
anonymity

pseudonymity
anonymity

pseudonymity
anonymity

pseudonymity

@feyleanor

English(INTp, hacker, author, physicist, musician, libertarian, goth, christian, tory, LgbT, digital identity) = Human(superior, sociable, contrarian, neophile)

Joined August 2007
“What’s in a name?
That which we call a rose,
by any other name would smell as sweet.”

William Shakespeare
SECURE TOKENS

➤ tokens alone are not proofs of the identity of their bearer

➤ a biometric needs to be captured to associate a token with an identifiable human being

➤ and the biometric must be confirmed by a person or an algorithmic process at the time identity is being asserted to perform an identification

➤ evidence that this has occurred should be recorded if this needs to be confirmed at a later date such as in a court of law
BIOMETRICS

➤ if it can be measured and tends towards uniqueness…

➤ faces
➤ fingerprints
➤ iris patterns
➤ retina patterns
➤ genetic fingerprints
➤ electrocardiogram
➤ electroencephalogram

➤ it can also be duplicated and counterfeited!
ID CARD

➤ photo for visual comparison
➤ hologram to assert validity
➤ date of birth reveals age
➤ serial number allows this card to be recorded and tracked
➤ physical security features increase the cost of counterfeiting
➤ smart card features allow a card to be used with digital scanners
➤ but how much scrutiny will be applied when the card is used?
LIVENESS

- digital data is easily copied
- replay attacks repeat a previously captured biometric
- spoofing creates a facsimile of a biometric capable of fooling a digital system
- proofs
  - is data being captured now
  - is it from a genuine source
  - has it been tampered with
  - is it likely to be unique
TRUST ARBITRATION

➤ a contract is an agreement to do something between two parties
➤ in Common Law this requires both intent and an exchange of consideration
➤ a contract can be enforced by the courts even if it has no written form
➤ trust relies on recognised authority and transparency of process
➤ the internet has no courts and machines lack intent so we must provide witnesses that a human decision was made and rely on off-line courts to resolve disputes
CHECKING IDENTITY

➤ each exchange of identity comes with proof that the exchange occurred
➤ proof engenders trust
➤ we anchor trust in information based on its provenance and its tamper-resistance
➤ we can also capture proof of why the exchange occurred
➤ we can record these proofs for future reference
➤ good bookkeeping is at the heart of all identity schemes
HMAC hashes are large numbers computed from a set of data with cryptography. Any change to the set of data will result in a different HMAC value being calculated. Symmetric encryption allows two parties with the same key to communicate securely. Public key encryption keeps the decryption key secret. Hybrid encryption allows a symmetric key to be shared as data by encrypting it with a public key.
UNIQUENESS

- a one-time pad is a single use key for encrypting a message
- it provides a unique mapping between the encrypted content and the keys to generate and recover that content
- it provides perfect secrecy as there are no variant encrypted texts which can reveal elements of the keys
- one-time pads require key management which guarantees uniqueness and randomness
IMMUTABILITY

➤ singly-linked lists are a popular abstraction in computer science

➤ they allow several lists to share common starting segments

➤ a hash chain extends this concept with computed hashes for each element and an optional signature to validate them

➤ alter one item in the chain and all subsequent hashes must be recalculated for the signature to remain valid
INTEGRITY

- Trees are another popular data structure related to lists but used to capture hierarchical structures and optimise search.
- Merkle trees are trees built from hash chains.
- Adding to the tree creates a new root element whose hash proves the integrity of its links and leaf elements.
- Building many overlapping trees ensures that changes to one tree will invalidate other trees.
- Bitcoin uses a hash chain of Merkle trees packaged as blocks of information to provide nonrepudiation.
- The hash chain can be forked deliberately or as a result of network partitioning.
- The Bitcoin consensus algorithm is based on proof of work which limits the rate at which transactions can be performed.
- And if forks are later merged together then the shorter fork is discarded.
- Forks can overcome this by using sidechains for exchange.
- the internet comprises a decentralised physical infrastructure
- most applications are built with a centralised client-server model which hides this reality
- servers act as trust anchors
- blockchain mining & etherium dApps are fully distributed
- lacking servers they require a consensus algorithm to agree a trusted reality
CASE STUDY: DESIGNING UPASS

patented by Yoti Ltd, 130 Fenchurch Street, London
PRINCIPLES

➤ UK common law identity
➤ functional anonymity
➤ resistant to mass surveillance
➤ a reliable source of information even if the information itself is unreliable
➤ transactions are fast with minimal need for consensus or protocol handshakes
➤ can be scaled to a global system
➤ works on desktop, mobile & IoT platforms
OVERVIEW

➤ an anchor document underlies each identity
➤ mobile-centric design
➤ everything happens on the handset
➤ QR codes for easy token sharing
➤ validation service
➤ check tokens
➤ release information
➤ secure store is an encrypted datastore
➤ one-directional flows share trust between all three actors
REGISTRATION

➤ digitise anchor document
➤ capture selfie
➤ create profiles
  ➤ anonymous
  ➤ date of birth
  ➤ name
  ➤ nationality
➤ generate encryption keys
➤ record phone address
➤ issue anonymous profile credential
TRANSACTIONS

➤ a customer presents a profile credential to a merchant
➤ the merchant adds a credential of their own
➤ both credentials are sent to validation server
➤ the validation server confirms the credentials are known to it
➤ it invalidates these and sends receipts directly to both customer and merchant
➤ the receipts provide fresh credentials
➤ only the server
➤ knows the delivery addresses
➤ can make fresh credentials
PROFILES

➤ a set of keys and their associated values
➤ essentially a web form
➤ anchored to a document or assigned by another profile
➤ has a confidence value based on its provenance and usage
➤ is immutable and links to previous versions of itself
➤ has an associated selfie chain with photos of its owner
➤ anonymity is represented by a profile containing no keys or values
CONFIDENCE

➤ courts reach a verdict by judging the relative credibility of evidence & witnesses

➤ a distributed ledger which is very difficult to tamper with provides a powerful witness

➤ and each anchor document is a witness of the profile data depending on it

➤ a profile’s associated selfie can be inspected by its recipient at the time the transaction takes place and compared with the presenter’s face

➤ combined with a confidence value this provides a reasonable basis for making informed choices
RECEIPTS

➤ receipts come in pairs
➤ each receipt has links to the relevant information about the other party
➤ links are included to the profile presented and to any profiles previously assigned by the recipient
➤ receipts are encrypted with a symmetric key specific to the profile used by the recipient
➤ and they contain a shared key which is unique to this transaction
➤ each receipt contains a link to the previous transaction performed by this profile
MASTER RECEIPTS

➤ receipt pairs are recorded opaquely as master receipts in the secure store

➤ a master receipt is encrypted with the shared transaction key

➤ the transaction key is never recorded in the secure store

➤ master receipts form a chain

➤ the index for this chain is calculated from the credentials used but these are only stored in the receipt pair
FACE RECOGNITION

- The human brain is generally good at looking for and identifying faces.
- Machines can be taught to match faces by reducing them to a templated form.
- This templated form can act as an index to return one associated identity among many.
- Or it can be associated with a particular profile and used to confirm identity.
- Each source image for the template and their order are recorded in a blockchain.
- This allows the template to be recalculated for any point in a profile's history.
to be practical a biometric should be simple to capture & tamper resistant

it should also have a differential property which can be used to test it's live

pupillary response to a succession of bright flashes of light has calculable properties

and eye movement may be guided using a shared cryptographic secret which will be unique to a particular device

the server sets the parameters randomly for each test making the results unique to this particular interaction
 DEVICE LIVENESS

- live biometric responses with random parameters give us unique values
- by controlling where and how these are delivered we can prove uniqueness of our current interaction
- as a result we can prove the device is live
- as with a transaction we use one-way messaging which can reduce the ability of an eavesdropper to apply flow analysis
Sometimes we need to perform transactions via an untrusted intermediary.

These are potentially subject to Man-in-the-Middle attacks.

By having a remote server use our device as a validator, we can perform a transaction and give them access to a secure back channel.

Now we can monitor & control their connection to our untrusted intermediary.

Essentially the remote site has to login to our local system.
ASSET TRACKING

➤ the building blocks of uPass can provide identity to things as well as people

➤ we can use this fact to create private identity spaces unique to a particular asset class such as event tickets

➤ this can be used to control how the asset changes hands