Yivi's attribute-based authentication, in perspective

Cybernetica seminar, Tallinn, Estonia

Bart Jacobs — Radboud University, Nijmegen, NL

bart@cs.ru.nl

Outline

Where we are, so far

Who is this guy?

- Professor of computer security & privacy at Nijmegen, NL
  - Member of Royal Netherlands Academy of Arts and Sciences
  - Recipient of Stevin premium 2021, highest award in science in NL
- Formal (0.0) appointment both at Philosophy and at Law faculty
  - co-founder of iHub for interdisciplinary research at Nijmegen
- Active in media, societal debates and parliamentary hearings
  - e.g. about digital sovereignty, intelligence etc.
- Non-renumerated chair of Privacy by Design foundation — which owns Yivi (and PubHubs) rights, see later
- **Anecdote**: I once said on a panel in Brussels next to former Estonian president Ilves and showed him Yivi ...
  - he said he was not interested, saying Estonian already had the best identity system in the world!
  - but: all European member states must have attribute-based wallets in 2026

Global platforms

VS	Europe	China
Google, Amazon, Uber, Apple, Airbnb, Netflix	Spotify	Baidu, Alibaba, Tencent

etc

EU / NL / Nijmegen / own perspective

- EU is regulatory power, but not a technology power
  - embedding EU values requires stronger digital autonomy
- Open source as a geopolitical instrument, to keep big-tech at bay
  - NL government has "open, unless" aims, not enforced
  - EU is only starting with European Digital Infrastructure Consortium (EDIC), focused on digital commons
  - Initiative of Ger, Fr, NL and Estonia!
- Nijmegen's interdisciplinary iHub for digitalisation and society
  - with value-driven research agenda and own development/design lab
- Own team projects with strong "usable security" focus:
  - Yivi.app, for attributed-based identity management
  - PostGuard.eu, for identity-based encrypted email & file transfer
  - PubHubs.net, for a new community network

Where we are, so far

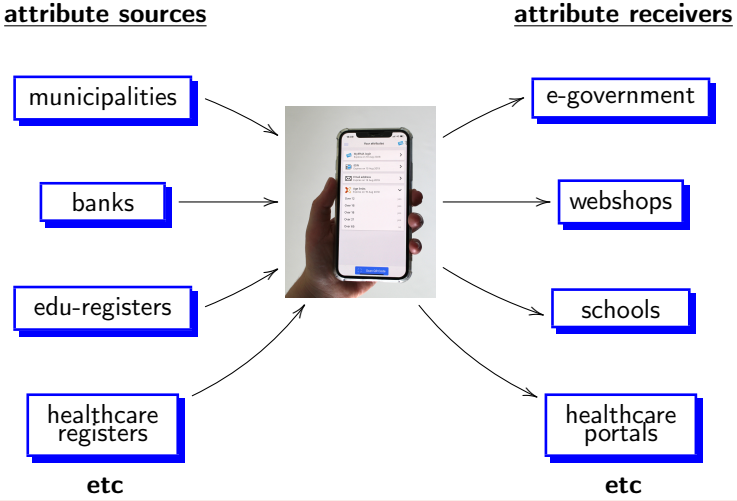
General remarks about Yivi

- Started around 2010, as academic research project, called "IRMA"
  - crypto-basis: zero-knowledge proofs, from Idemix (IBM, Zürich)
  - also for identifying attributes, like full name, email, mobile nr.
  - with smart card (first) and phone app (later) prototypes
  - new concept: proportional authentication — with data minimalisation
- In 2015 IRMA moved out of academia, to non-profit spin-off
  - called privacybydesign.foundation
  - roll-out 2019-24 with SIDN, non-profit domain registrar in NL
  - 2024-now, with commercial company Caesar Group (see later)
  - some academic Yivi research remains at university, e.g. PostGuard
  - Yivi has $\geq 100K$ users, but no (inter)national breakthrough
- Hugely influential, e.g. copied by EU in their wallet-ID plans
  - working app has been eye-opener for policy makers & others
  - **Message**: things can be done differently, there is a (political) choice, esp. relevant now for EU digital sovereignty.

Current cooperation with company Caesar

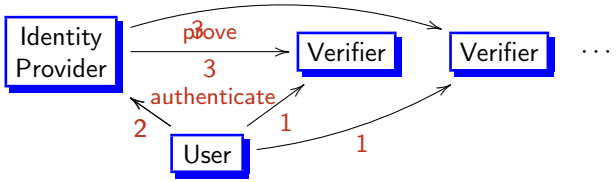
- The privacy by design foundation holds Yivi brand rights
  - and also web addresses like yivi.app and yivi.nl
  - the foundation does *not* have own employees
- Caesar is family-owned, Dutch IT-company, with ±150 employees
- The foundation and Caesar have signed a contract, saying in essence:
  - Caesar gets exclusive rights to (commercially) exploit Yivi brand
  - they run the infrastructure (backend servers, app) with EU hosting
  - they keep Yivi open source, privacy-friendly & secure, free for end-users
  - strategic decisions are taken jointly.
- The aim is to combine public values with corporate efficiency
  - this works well, so far

The Yivi app as everyone's personal hub

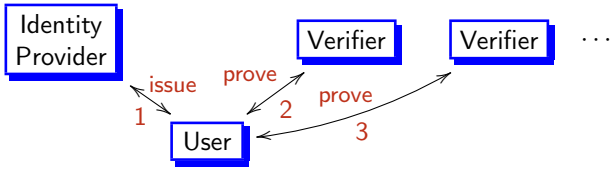


Centralised versus decentralised, schematically

Centralised: everything goes via the Identity Provider (e.g. Facebook, Itsme)



Decentralised: everyting goes via the User (think Yivi)



Note: Data flows determine power relations in modern societies!

Yivi security guarantees

- Non-transferability: my little nephew should not be able to get my "over 18" attribute (and go to XXX sites)
  - realised via binding to personal private key
- Issuer-unlinkability: the issuers should not be able to track where I use which attributes
  - realised via blind signature on credentials
- Multi-show unlinkability: service providers should not be able to connect usage (at different providers)
  - realised via zero-knowledge proofs
- Revocation: outdated attributes should be blockable.
  - most difficult, partly in conflict with previous requirements
  - solution using one-day *epochs* implemented, but not in use.

Yivi ecosystem & applications

- Some tensions with national NL government: Yivi poached on their turf
  - Ministery of Internal affairs thinks it "owns" (digital) identity
  - however, it is very slow to act; Yivi is more innovative
  - it treats Yivi as a commercial supplier, not as a partner
  - it cannot deal with/integrate societal open source developments
- Several applications by local government
  - esp. city of Nijmegen allows Yivi login, for citizens & business
- Other applications in insurance and health care
  - several more parties are experimenting
  - difficult for them to decide, given various, non-consistent national & EU developments
- It is difficult to get the eco system gets off the ground
  - hardly any incentives for commercial organisations: overhead
  - works best when there is an identity-check obligation
  - e.g. for age limits (≥ 16, ≥ 18), but no broad adoption yet

Yivi business model

Recall: Yivi disclosures are directly between end-user (phone) and verifier ('relying party')

- there is not intermediate party who can keep track, count, charge
- also: anyone can use Yivi as verifier

Two sources of income are currently explored:

(1) Via Identity brokers; in NL they all support Yivi.
  - They can count — and are privacy hotspots
  - part of their charges goes to Yivi

(2) Via registration of verified verifiers — for a price
  - User will get a warning in the Yivi app if they are about to disclose to a non-verified verifier (relying party)
  - this can work via a flat fee
  - (there will be special arrangements for non-profit verifiers)

Where we are, so far

Napoleon's heritage: completely different mindsets

- It was Napoleon who started registering people's identities in the countries that he conquered
- He needed these registers to draft people into his huge armies
- This never happened in Anglo-Saxon countries — which typically have no citizen administration
- People in continental Europe, in contrast, see the government as the primary source of (administrative) identities
- In the Anglo-Saxon world there is much more identity anarchy
  - you need energy & phone bills etc. to prove who you are
  - in the US a state-issued driver's licence works best as identity

National differences/traditions/sensitivities

- Substantial differences exist within Europe:
  - GB & DE have no national citizen identification number
  - NL has a national identification number — for public use only
  - Scandinavian & Baltic countries do have such numbers — for both public and private usage
- With such ubiquitous numbers, digital identity management is easy
  - but it introduces many privacy concerns
  - buying alcohol in Swedish shops involves citizen identity registration
  - Estonia chooses transparancy over privacy
- Attribute-based identities can accomodate such national differences
  - altough an EU-wide system does require some commonality

EUDI-wallet compliance

- EUDI-wallet = European Digital wallet, announced in 2021?
  - part of EU sovereignty initiative
- Technical details in Architecture Reference Framework (ARF)
  - zero-knowledge proofs (ZKPs) are not included
  - standard ECDSA signature are used, making people traceable
  - partial fix: issue multiple versions of the same credentials
- Much criticism and debate about ARF, see e.g.
  - Cryptographers' Feedback on the EU Digital Identity's ARF
- Why stick with old crypto? Mainly:
  - ZKP is not (sufficiently) standardised — security proofs do exist
  - crypto algorithms need hardware support
- ARF is moving target, now at version 1.5, published early feb.'25
  - Multi show / issuer unlinkability are now identified as challenges
  - will be dealt with in version 2.0 — via ZKP?

Dilemma for Yivi

- Yivi currently runs most privacy-friendly crypto
  - Idemix ZKP, with Camenisch-Lysyanskaya signatures (via RSA)
  - ZKP-implementatation could be updated to BBS'04 (on curve)
  - ARF-compliance would be step back
- Still, ARF-compliance is needed for wide-scale adoption. Dilemma:
  (1) comply now to (moving) standard, with bad crypto
  (2) stick to own good crypto, for the time being
- Chosen approach — but not implemented yet — crypto agility
  - support for multiple crypto systems in Yivi
  - negotiation between verifier and app about what is available
  - requires issuers to provide multiply signed credentials
  - introduces extra complexity and new attack vectors
- Crypto agility does provide basis for post-quantum versions!
  - In EU-proposal, and in new zkDilithium for Yivi by Ádám Vécsi

Where we are, so far

Basic observations

- Email encryption exists for decades, but is hardly used
  - most well-known: PGP
  - only 0.06% encrypted, out of 82 million analysed mails
    (Stransky et al. https://doi.ieeecomputersociety.org/10.1109/SP46214.2022.9833755)
  - "manual key management is unusable for novice users"
    (Ruoti at al. https://dl.acm.org/doi/10.1145/3313761)

- Many variations exist, with both local and central key storage
  - popular in NL: portal-based approaches, like *Zorgmail*, where one party stores all messages — aarghh!
- GDPR pressure increases
  - passport copies via email is getting unacceptable
  - easy-to-use solutions are needed, for the masses
  - PostGuard idea: combine identity-based encryption (IBE) and Yivi

PostGuard: a bird's eye view

- **Sender** chooses artributes of receiver and forms associated public key
  - using master public key
- **Receiver** discloses relevant attributes to central Private Key Generator (PKG) and gets associated private key to decrypt.
  - attribute disclosure works via Yivi
- Underlying mental model — since "encryption" is too difficult
  - PostGuard explanation: only the intended recipient can read
  - confidentiality is reduced to authentication
- Prototype implementation is up-and-running
  - try yourself postguard.eu
  - also includes attribute-based signatures
- PostGuard illustrates what identity-wallets can enable.

Where we are, so far

PubHubs motivation, outline

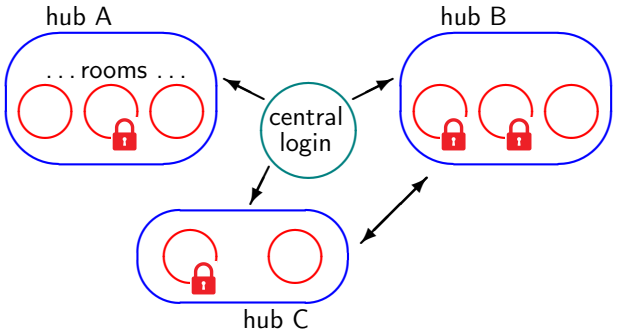
- Current "social" networks have devasting societal effects
  - fake news, extremism, polaristion, all via engagment optimisation
- PubHubs is non-profit, from civil society, based on public values
  - its design should encourage people to behave more civilised
  - it aims to combine privacy and accountability
- PubHubs has a central login, forming an umbrella over local hubs
  - conversations take place locally, in hubs
  - hubs are run by schools, hospitals, libraries, municipalities, etc.
  - these organisations moderate their own hub
  - users have (persistent) pseudonyms, different per hub
  - hubs form local data and name spaces
  - implemented as enhanced Matrix servers

PubHubs and digital identity

- Digital identity is a crucial part of PubHubs
  - for central login, and also for "secure" rooms in hubs
  - e.g. for disclosing your postal code for neighboorhood room
- Identity is an instrument for moderation, and accountability
  - e.g. a misbehaving user may need to disclose their real name
  - ultimately it is used for exclusion — requiring persistency
  - users may be banned from rooms / hubs / PubHubs
- Therefore, standard social logins do not work for PubHubs
  - also, Matrix logins do not give access
  - nor Fediverse / ActivityPub

See *PubHubs Identity Management* publication: doi.org/10.1093/logcom/exad062

PubHubs high-level picture



- Once logged in (centrally), users can freely move between hubs
- Users automatically get different pseudonyms in different rooms
- Access restrictions may apply to rooms within hubs
- This infrastructure is up-and-running

Final topic: the authenticity crisis

- Concerns exist today about artificially generated content and dis-/mis-information — and their societally destabilising effect
- Veracity of information is unsolvable, esp. in political matters
  - fact checking provides limited help to citizens
- Authenticity is a more helpful concept
  - it involves certainty about source and integrity of messages
  - it can be guaranteed technically, via digital signatures
- Digital signatures are useful tools for people to make their own credibility and veracity judgements
  - signatures can strengthen institutions online — when they start signing

See BJ, *The Authenticity Crisis*, Computer Law & Security Review 53, 2024, doi.org/10.1016/j.clsr.2024.105962

Where we are, so far

Concluding remarks

- Yivi has a rich history as front-runner wallet app
  - hugh impact of academic work — via EU wallet framework
  - Yivi wallet implementation has opened eyes: aha, now I see
  - decentralised & open source set-up not always copied
- Acutal, wide-scale adoption meets many practical challenges
  - hardly any commercial incentives; regulation does help
  - standards uncertainties — crypto agility as possible answer
  - joining forces with other countries helps
- Digital identity is enabler for many applications, to harden our digital infrastructure
  - e.g. PostGuard / PubHubs
  - digital signatures for authenticity
  - but also e.g. in online voting & decision making
- *Cri de coeur*: we need structural support in EU for open source software development — as now tried via EDIC

Thanks for your attention. Questions/remarks?