Revocable Anonymous Credentials
from Attribute-Based Encryption

Giovanni Bartolomeo

CNIT

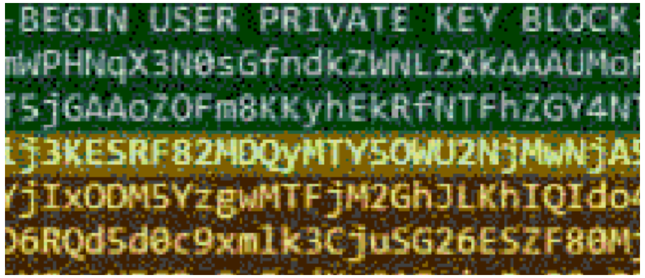
(giovanni.bartolomeo AT uniroma2.it)

Hello!

1. About myself: https://www.linkedin.com/in/giovannibartolomeo/

consorzio nazionale interuniversitario per le telecomunicazioni

2. About CNIT: https://www.cnit.it/



3. Some resources about this work:
   https://github.com/netgroup/abe4jwt
   https://arxiv.org/html/2308.06797v3

Why this work?

1. Digital Identity is a very hot topic today, however…

2. Broken Access Control was ranked OSWAP#1 Application Security Risk in 2021. OSWAP#2 is Cryptographic Failures (i.e., lack of or misuse of crypto algorithms)

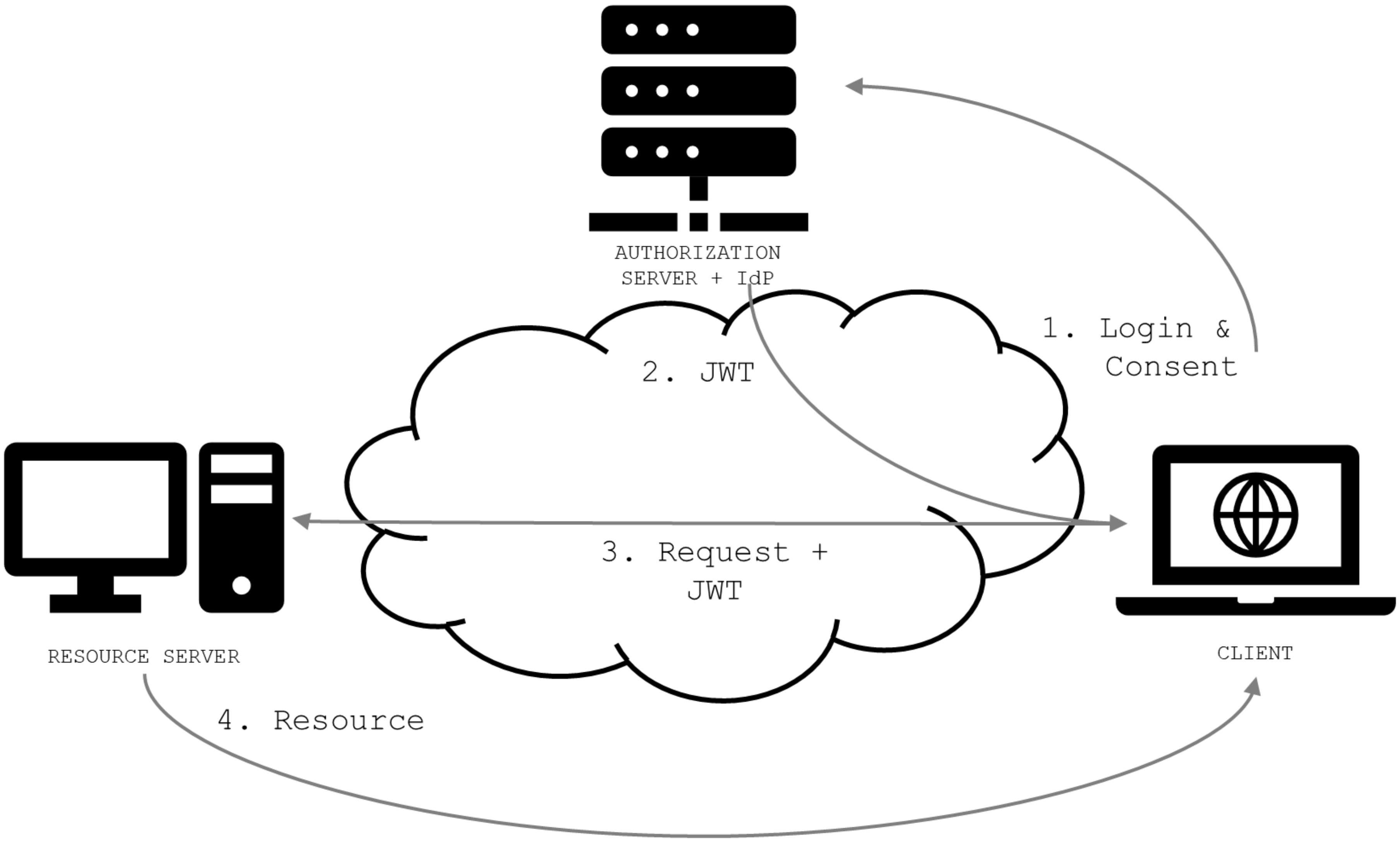
3. IdM related products and specs are progressively increasing their complexity as new vulnerabilities are found and newly desired features are introduced

4. Moving most access control functions from software to math might enable a simpler and effective security design

An ideal AC flow (OAuth Implicit Grant).

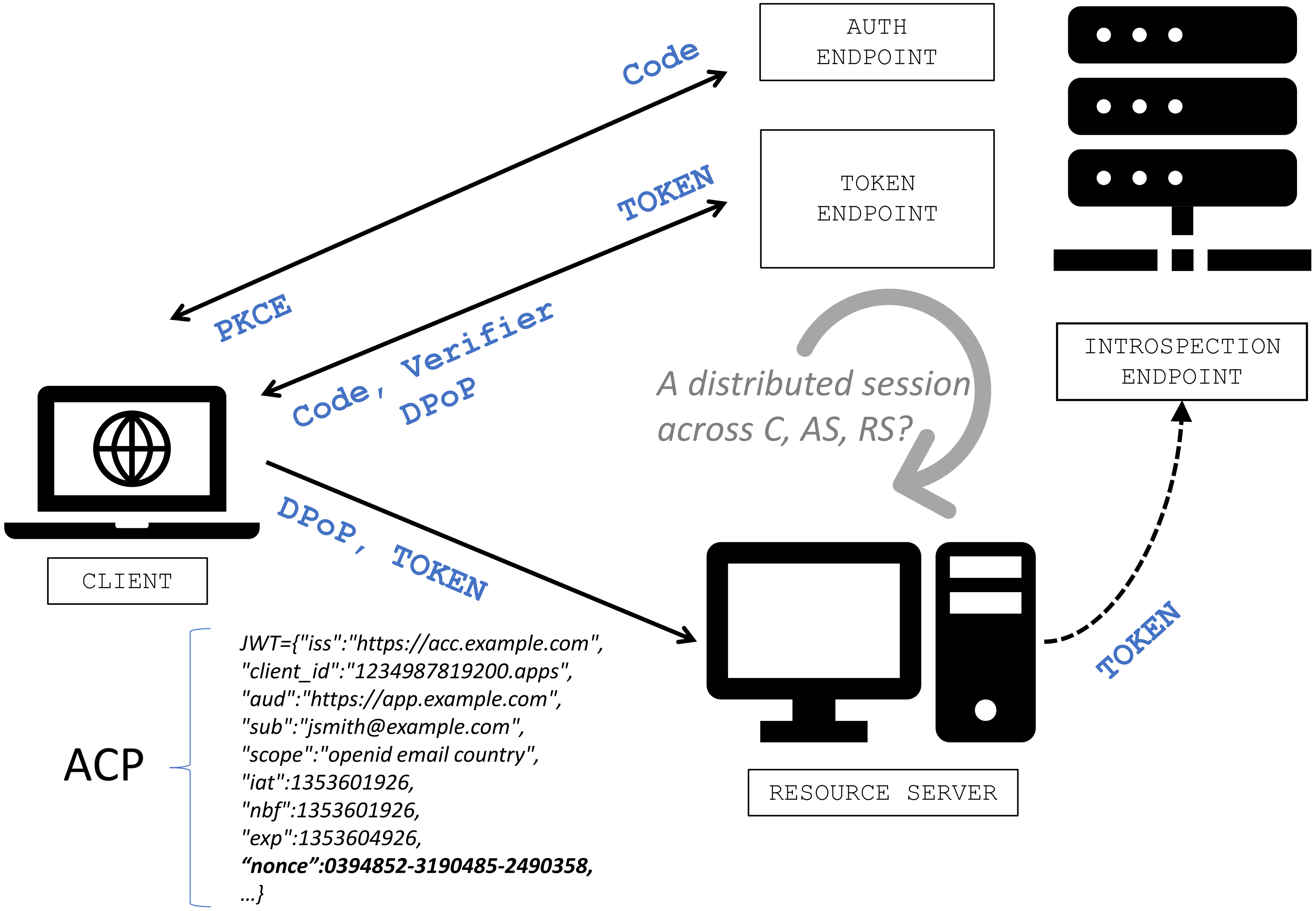
*Interesting part of the protocol under investigation is the **authz req and res**, which happens through http GET cross site/server side requests.*

Implicit Grant is unsecure as parameters are carried en clair as URL in the authz req/res.



Open ID Connect flow using current best practices

Access control is implemented in a mix of crypto-primitives and code

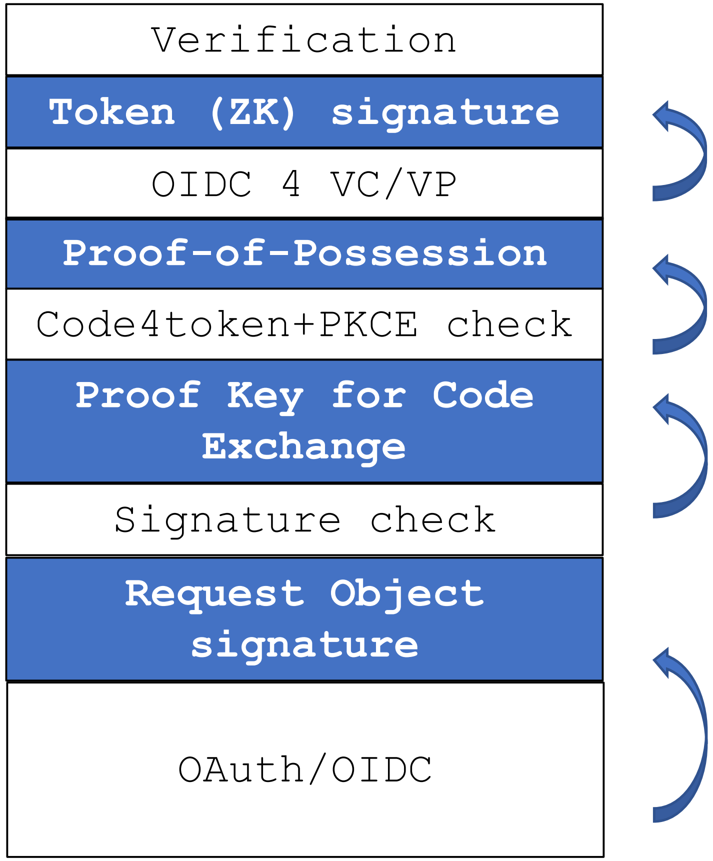


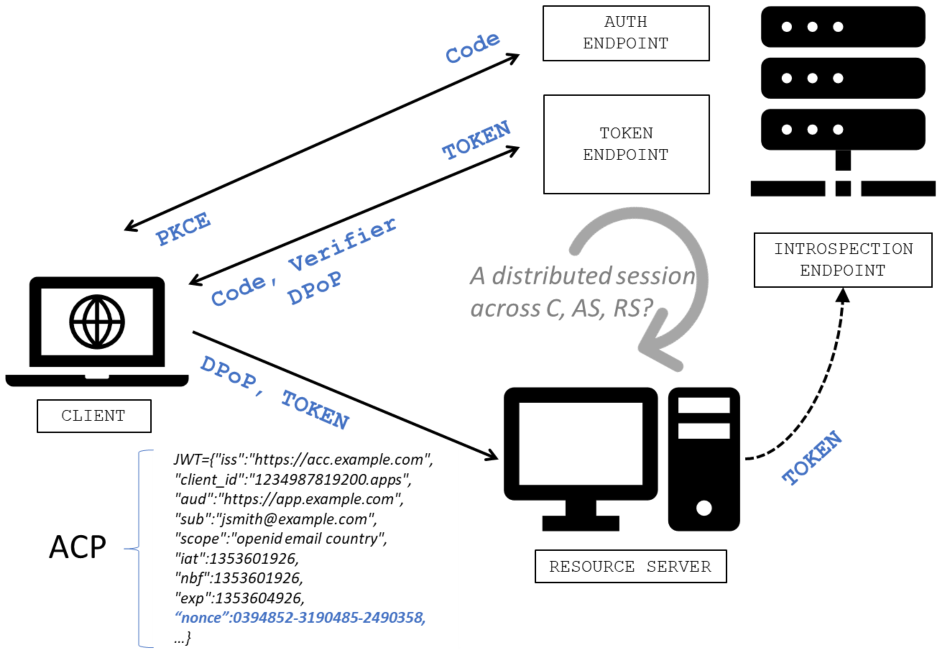
Open ID Connect flow using current best practices

Access control is implemented in a mix of crypto-primitives and code

Developer needs a continous hop on/hop off from code to crypto and viceversa

Code needs to be inspected and certified for correctness





Predicate Encryption

Public Key Crypto	Identity-Based Encryption[1]	Attribute-Based Encryption[2-4]
$z=\{x\}_{pk(a)}$	$z=\{x\}_{mpk,\text{"receiver"}}$	$z=\{x\}_{mpk,(a\wedge b)\vee c}$
$x=\{z\}^{-1}_{sk(a)}$	$x=\{z\}^{-1}_{mpk,sk(\text{"receiver"})}$	$x=\{z\}^{-1}_{mpk,sk(\{a,b\})}$
Solves key-distribution problem (pk is publicly available)	*Many randomized secrets keys for one set of MPK, MSK*	*Combines IBE with SSS [2] and monotonic span trees [3,4]*
	Public keys "replaced" by plain strings	*A fine-granuled content access policy implemented in crypto!*
	A KMS distributes MPK and generates secret keys	*Many other math properties…*

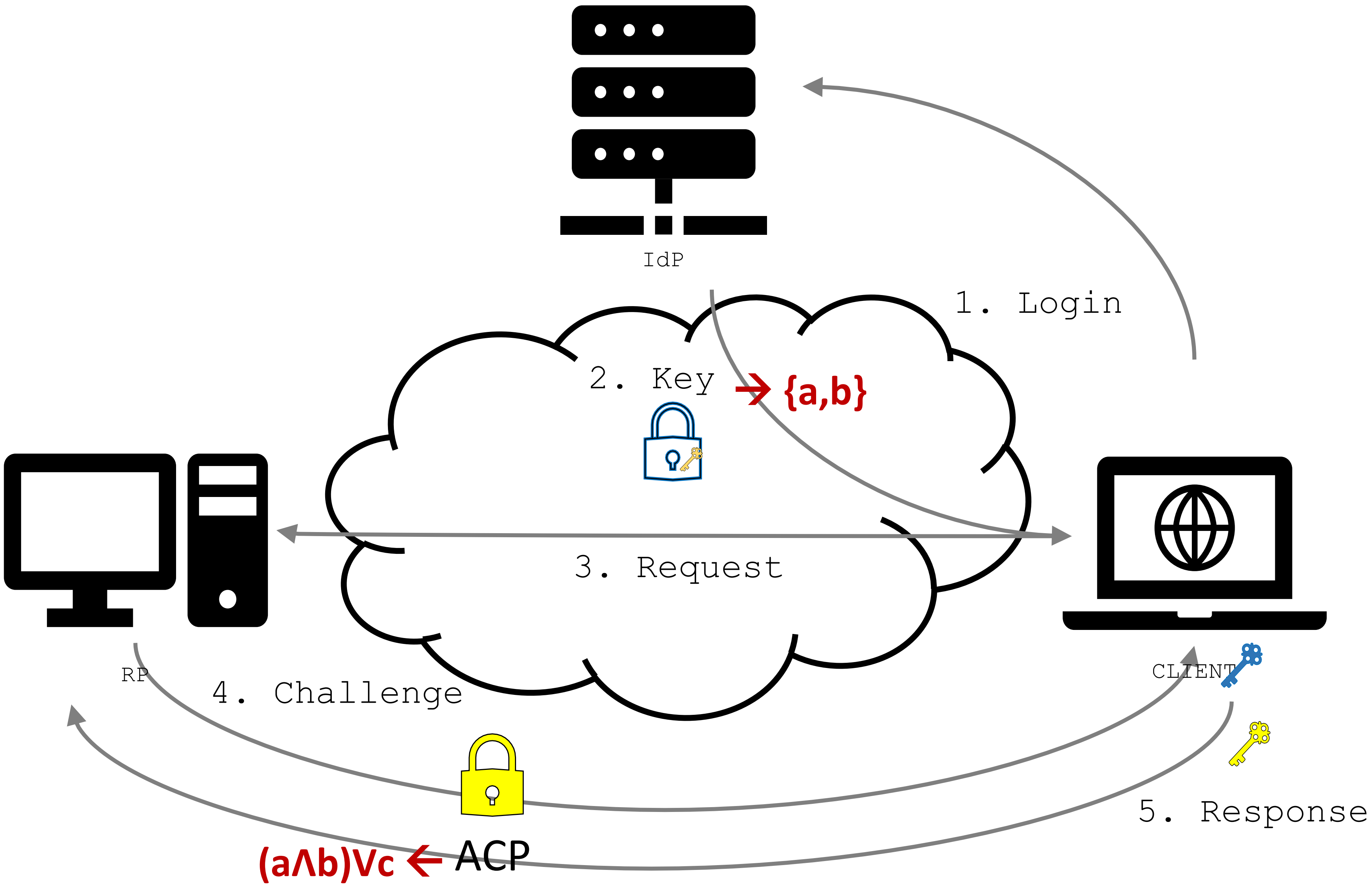
1. A. Shamir. Identity-based cryptosystems and signature schemes. In Proceedings of CRYPTO 84 on Advances in cryptology, pages 47–53. Springer-Verlag New York, Inc., 1984.
2. A. Sahai and B. Waters. Fuzzy identity-based encryption. In EUROCRYPT, pages 457-473, 2005.
3. V. Goyal, O. Pandey, A. Sahai, B. Waters: "Attribute-based encryption for fine-grained access control of encrypted data", Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS '06, pages 8-98, New York, NY, USA, 2006. ACM.
4. J. Bethencourt, A. Sahai, B. Waters: "Ciphertext-policy attribute-based en-cryption", Proceedings of the 2007 IEEE Symposium on Security and Privacy, SP'07, pages 32-334. Washington, DC, USA, IEEE Computer Society.

Using Ciphertext Policy – Attribute-Based Encryption

Straightforward to implement

Less certification costs

Access control decision mostly enforced by proven math algorithms, not by code



Using Ciphertext Policy – Attribute-Based Encryption

Straightforward to implement

Less certification costs

Access control decision mostly enforced by proven math algorithms, not by code

```
Actions:

C    ->RS   : Scope
RS*  ->C    : as,{{Challenge}h(C,as,RS,Scope)}pk(C) #401 Unauthorized

C    ->as   : C,RS,Scope,Nonce
as   ->C    : {inv(h(C,as,RS,Scope)),Nonce}pk(C) #JWT containing an ABE key and a Nonce
encrypted to C

[C]*->*RS : Scope,Challenge,Session
RS* ->*[C]: Data,Session
```

Model checked using [1], formally correct with respect to the original goals

```
Goals:

C authenticates as on C,RS,Scope,Nonce #Nonce from as avoids a MITM attack
RS authenticates C on Challenge
C authenticates RS on Data
Data secret between RS,C
```

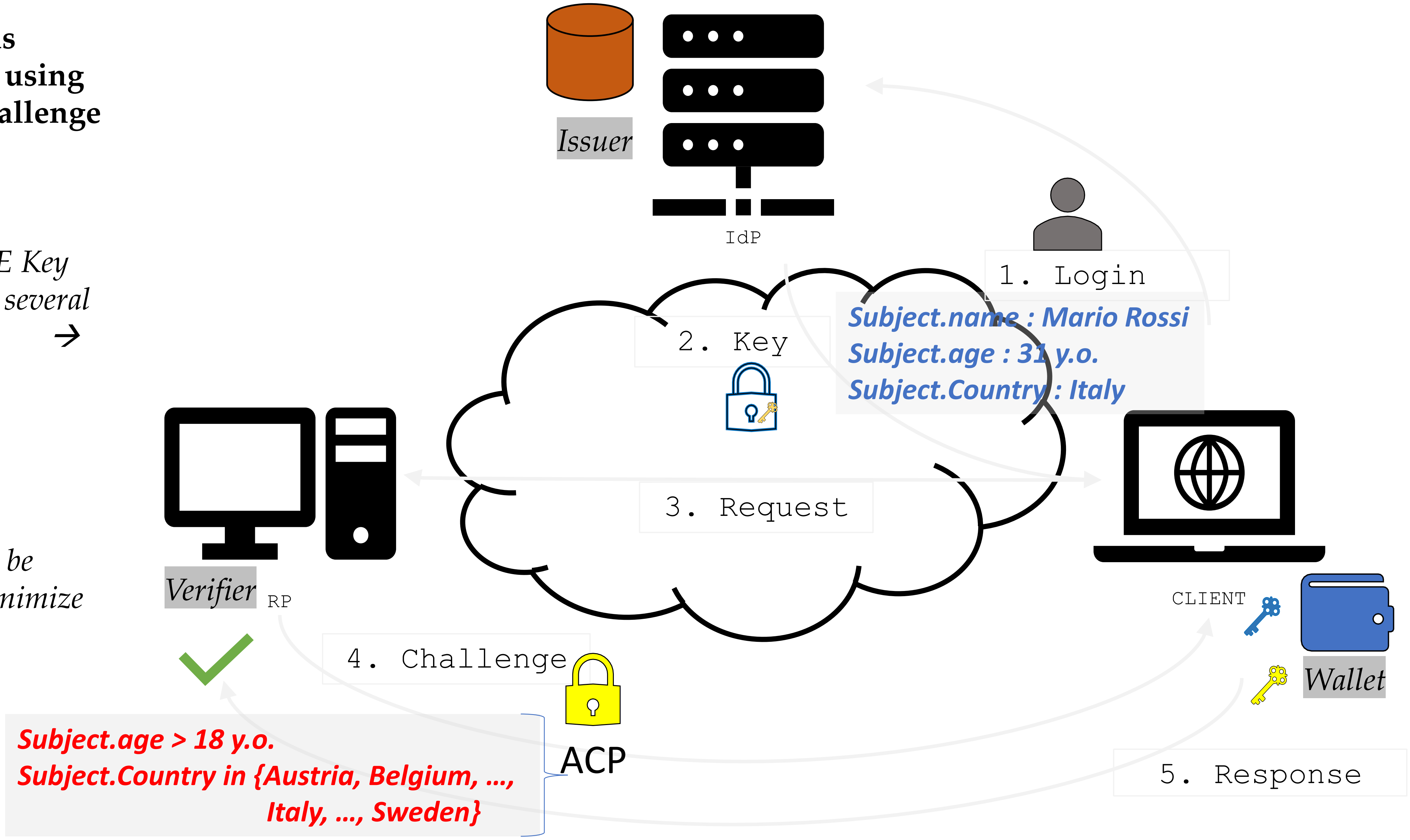
1. Basin, D., Mödersheim, S. & Viganò, L. OFMC: A symbolic model checker for security protocols. Int J Inf Secur 4, 181–208 (2005). https://doi.org/10.1007/s10207-004-0055-7

Anonymous credentials using CP-ABE challenge /response

A single ABE Key may contain several attributes… →

BUT

…policy can be shaped to minimize the needed knowledge →



Now, some questions…

1. *How to implement revocation?*
2. *Is ABE really Zero-Knowledge?*

…Back to drawing desk…

CP-WATERS-KEM plus Accumulators

We combined an early CP-ABE construction [1] with Camenisch's accumulator [2]

1. The algorithm associates an index to each new generated secret decryption key *K[i]*. The new index *i* is added to the accumulator *V*.
2. When the Authority needs to revoke a key, it simply removes the corresponding index *i* from *V* and updates the accumulator value.
3. With the addition or removal of elements to the accumulator, previously released keys become stale. Any party who has a valid key performs an update (the algorithm is locally executed without any secret or computation by the Authority).
4. The Authority updates the *MPK*.

```
//original CP-WATERS-KEM
Setup() → MSK,MPK
KeyGen(MPK,MSK,attr[]) → K[i],MPK
Encrypt(MPK,policy,secret) → C
Decrypt(MPK,K[i],C) → secret

//additional steps introduced by the accumulator
KeyRemove(MPK,i) → MPK
WitUpdate(K[i]) → K[i]
```

1. Waters, B. (2011). Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization
2. Jan Camenisch, Markulf Kohlweiss, and Claudio Soriente. 2008.An Accumulator Based on Bilinear Maps and Efficient Revocation for Anonymous Credentials.Cryptology ePrint Archive, Paper 2008/539.

Zero Knowledge Schemas

A Zero Knowledge schema, other than being complete and sound, guarantees that no verifier (statistically) learns anything other than the fact that a true statement is true.

Need: minimize disclosed information to preserve privacy

```
SK         = KeyGen(IKM, keyInfo);
PK         = SkToPk(SK);
signature = Sign(SK, PK, header, messages);
result     = Verify(PK, signature, header, messages);
proof      = ProofGen(PK, signature, header, ph, messages,
        disclosedIndexes);
result     = ProofVerify(PK, proof, messages.length, header, ph,
          disclosedMessages, disclosedIndexes);
```

An example: BBS signature [1] →

Pairing-based ECC signature that signs multiple messages (i.e., claims in a token). The signature and messages can be used to create a zero-knowledge proof of knowledge in which the original signature is not revealed, and messages can be selectively disclosed.

Efficient: only 2 pairings for verification: $\mathsf{e}(\overline{A}, X_2) = \mathsf{e}(\overline{B}, g_2)$

Limitations of BBS as PET: only support selective disclosure, **no support for predicates, membership proof or range proof** (Section 5.3 of [2])

1. S. Tessaro and C. Zhu.Revisiting BBS Signatures.Cryptology ePrint Archive, Paper 2023/275 https://eprint.iacr.org/2023/275
2. T. Looker, V. Kalos, A. Whitehead, M. Lodder, The BBS Signature Scheme, draft-irtf-cfrg-bbs-signatures-05, https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-signatures/

Proving the ZK conjecture for CP-WATERS-KEM…

Inspired by [1], we reuse part of the proof by Brent Waters for CCA Transformation [2]

*- Hardness of finding a forged C decrypting to some value M′ for a given SK is the probability of guessing C without knowing randomness **u** (with **u** ≠ u′)*

- *Hard for any attacker (including a dishonest Verifier)* → ***CCA secure***

- *C is uniformly distributed when K is chosen by the Verifier and r is chosen by the Prover* → **zero-knowledge**

$\mathbf{Encrypt}_{\mathbf{CCA\_KEM}}(\mathrm{PK}, \mathbb{A}) \to (K, C)$.

1. Choose random $K \in \{0,1\}^n$
2. Choose random $r \in \{0,1\}^n$ and let $u = H(r||K||\mathbb{A})$.
3. Run $\mathbf{Encrypt}_{\mathbf{CPA'}}(\mathrm{PK}, \mathbb{A}, M = (K, r); u) \to C$.
4. Output the key K, and ciphertext C.

$\mathbf{Decrypt}_{\mathbf{CCA\_KEM}}(\mathrm{PK}, \mathrm{SK}, C) = K' \cup \bot$.

1. Run $\mathbf{Decrypt}_{\mathbf{CPA'}}(\mathrm{SK}, C) = M' = (K', r')$
2. $\mathbb{A}' = \mathbf{ExtractAccessStructure}(\mathrm{PK}, C)$.
3. Let $u' = H(r'||K'||\mathbb{A}')$.
4. Run $\mathbf{Encrypt}_{\mathbf{CPA'}}(\mathrm{PK}, \mathbb{A}', M' = (K', r'); u') \to C'$.
5. Check $C' \stackrel{?}{=} C$ and if equal, output K'. Otherwise, output $\bot$.

1. Deuber, Dominic & Maffei, Matteo & Malavolta, Giulio & Rabkin, Max & Schröder, Dominique & Simkin, Mark. (2018). Functional Credentials. Proceedings on Privacy Enhancing Technologies. 2018. 10.1515/popets-2018-0013.
2. Brent Waters and Matthew Green. 2018.The OpenABE Design Document.Technical Report. Zeutro LLC Encryption and Data Security. https://github.com/zeutro/openabe/blob/master/docs/libopenabe-v1.0.0-design-doc.pdf

Takeaway

1. New challenges (e.g., verifier/issuer unlinkability) and discovered vulnerabilities imply increasing complexity for IdM protocols
2. Advanced crypto schemas such as Predicate Encryption may provide newly desired security features while streamlining design and verification
3. Leveraging on ABE, we combined rich policy expressiveness, efficient revocation (from accumulator) and anonymous proof of predicates over attributes into a single framework
4. The present contribution is a PoC!

Current limitations: PBC, RO model, # of pairings, negations, …

More info about Identity-Based and Attribute-Based Encryption

→

ETSI Security Week 2020 goes virtual!

Even More Advanced Cryptography

ETSI Standardization in Advanced Cryptography

Presented by: François Ambrosini, Umlaut
Christoph Striecks, AIT Austrian Institute of Technology

https://www.brighttalk.com/webcast/12761/409316

…but not for this talk ☺

THANKS!