EBERHARD KARLS UNIVERSITÄT TÜBINGEN

FACULTY OF SCIENCE
Communication Networks

End-to-End User Authentication with OpenID Connect: Use Cases and Benefits

by Jonas Primbs, Chair of Communication Networks, Faculty of Science, University of Tübingen, Germany

in /in/jonasprimbs

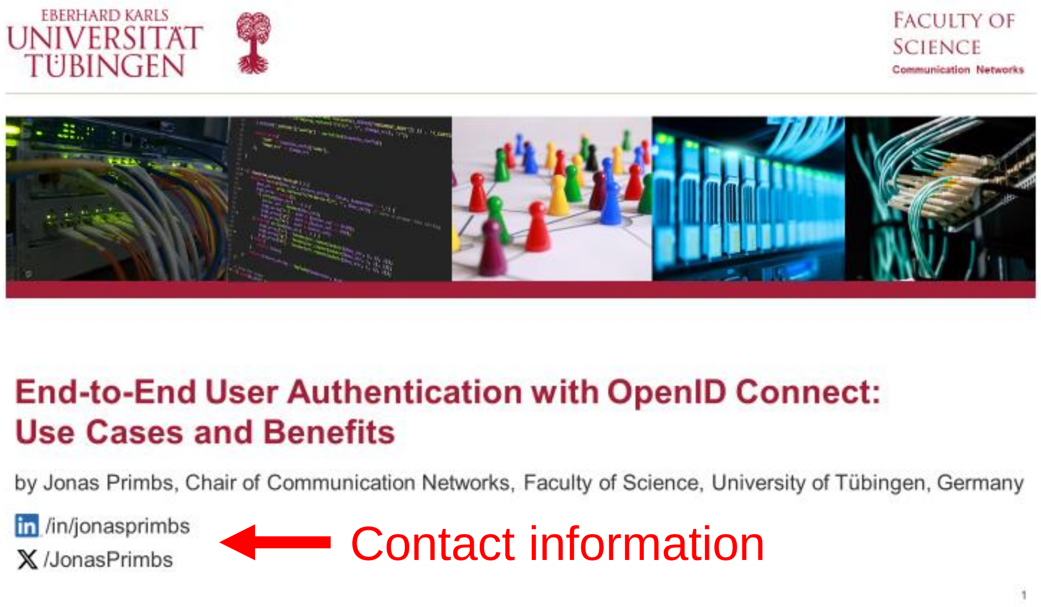
𝕏 /JonasPrimbs

http://kn.inf.uni-tuebingen.de

Introduction

- Assume a follow-up email conversation with me:
  - How can you be sure that this is really me?

- Remember contact info from first slide:



EBERHARD KARLS UNIVERSITÄT TÜBINGEN

FACULTY OF SCIENCE
Communication Networks

End-to-End User Authentication with OpenID Connect: Use Cases and Benefits

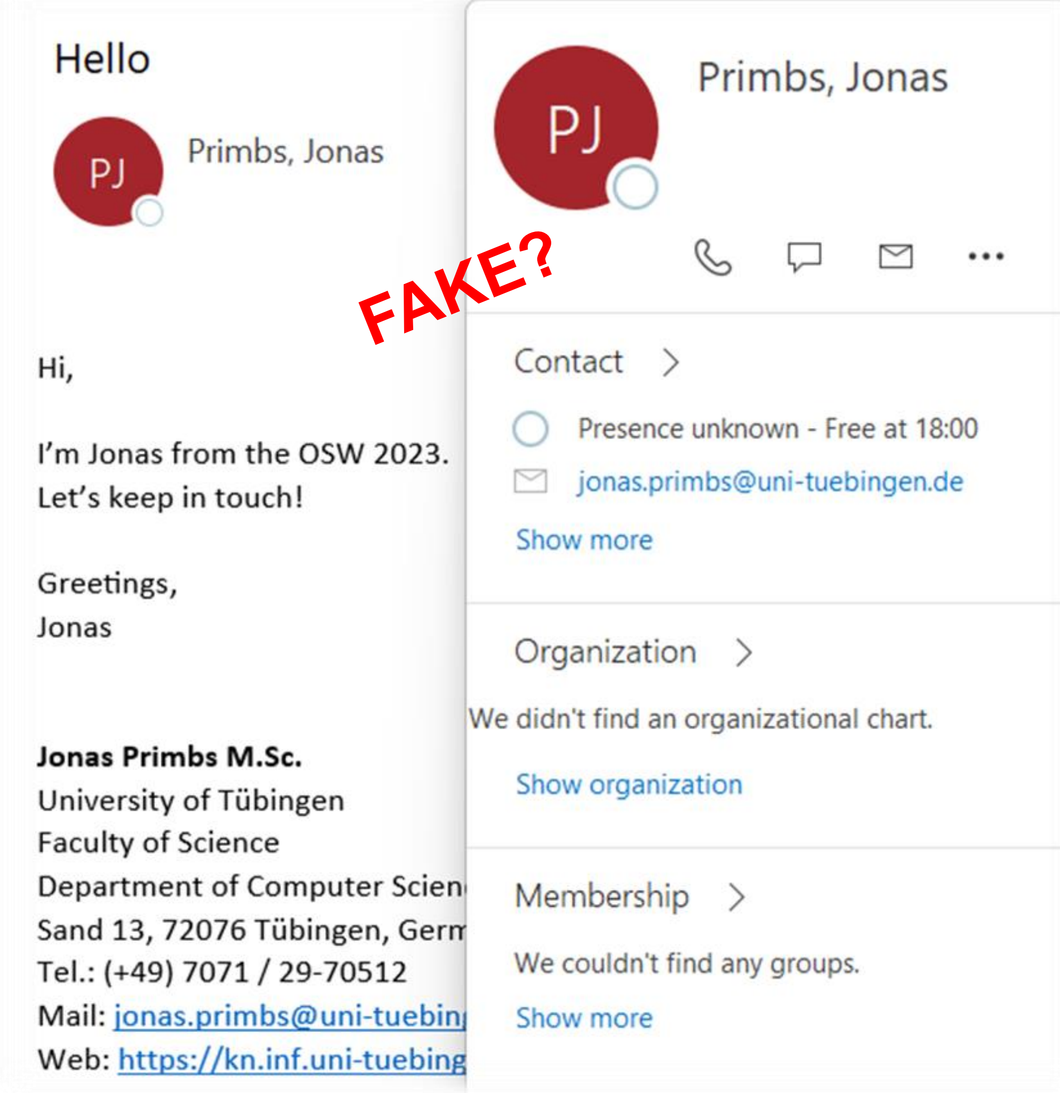
by Jonas Primbs, Chair of Communication Networks, Faculty of Science, University of Tübingen, Germany

in /in/jonasprimbs
X /JonasPrimbs

1

Contact information

- Goal: use OIDC accounts for end-to-end authentication



Hello

Primbs, Jonas

Hi,

I'm Jonas from the OSW 2023.
Let's keep in touch!

Greetings,
Jonas

Jonas Primbs M.Sc.
University of Tübingen
Faculty of Science
Department of Computer Scien
Sand 13, 72076 Tübingen, Germ
Tel.: (+49) 7071 / 29-70512
Mail: jonas.primbs@uni-tuebin
Web: https://kn.inf.uni-tuebing

FAKE?

Primbs, Jonas

Contact >

○ Presence unknown - Free at 18:00

✉ jonas.primbs@uni-tuebingen.de

Show more

Organization >

We didn't find an organizational chart.

Show organization

Membership >

We couldn't find any groups.

Show more

EBERHARD KARLS UNIVERSITÄT TÜBINGEN

FACULTY OF SCIENCE
Communication Networks

Message Layer Authentication with OpenID Connect

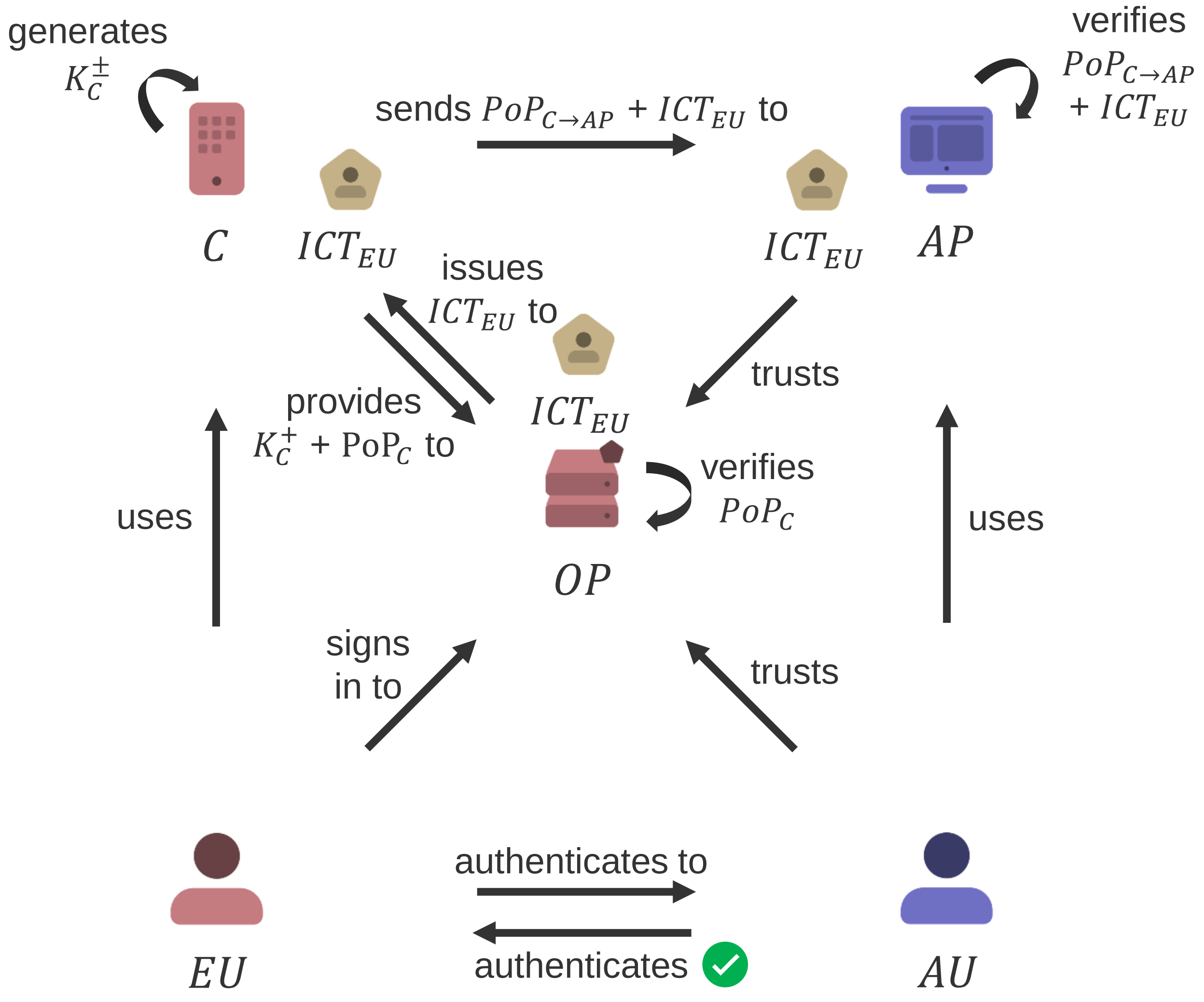
by Jonas Primbs, Chair of Communication Networks, Faculty of Science, University of Tübingen, Germany

http://kn.inf.uni-tuebingen.de

OAuth Security Workshop 2022

Trondheim, Norway

Recap + Update: Terminology



generates $K_C^{\pm}$

C

ICT_{EU}

sends $PoP_{C\rightarrow AP}$ + ICT_{EU} to

ICT_{EU}

AP

verifies $PoP_{C\rightarrow AP}$ + ICT_{EU}

issues ICT_{EU} to

ICT_{EU}

trusts

provides K_C^+ + PoP_C to

uses

verifies PoP_C

OP

uses

signs in to

trusts

EU

authenticates to

authenticates ✓

AU

End User (EU)
Resource Owner / real person

Client (C)
Client application of the EU

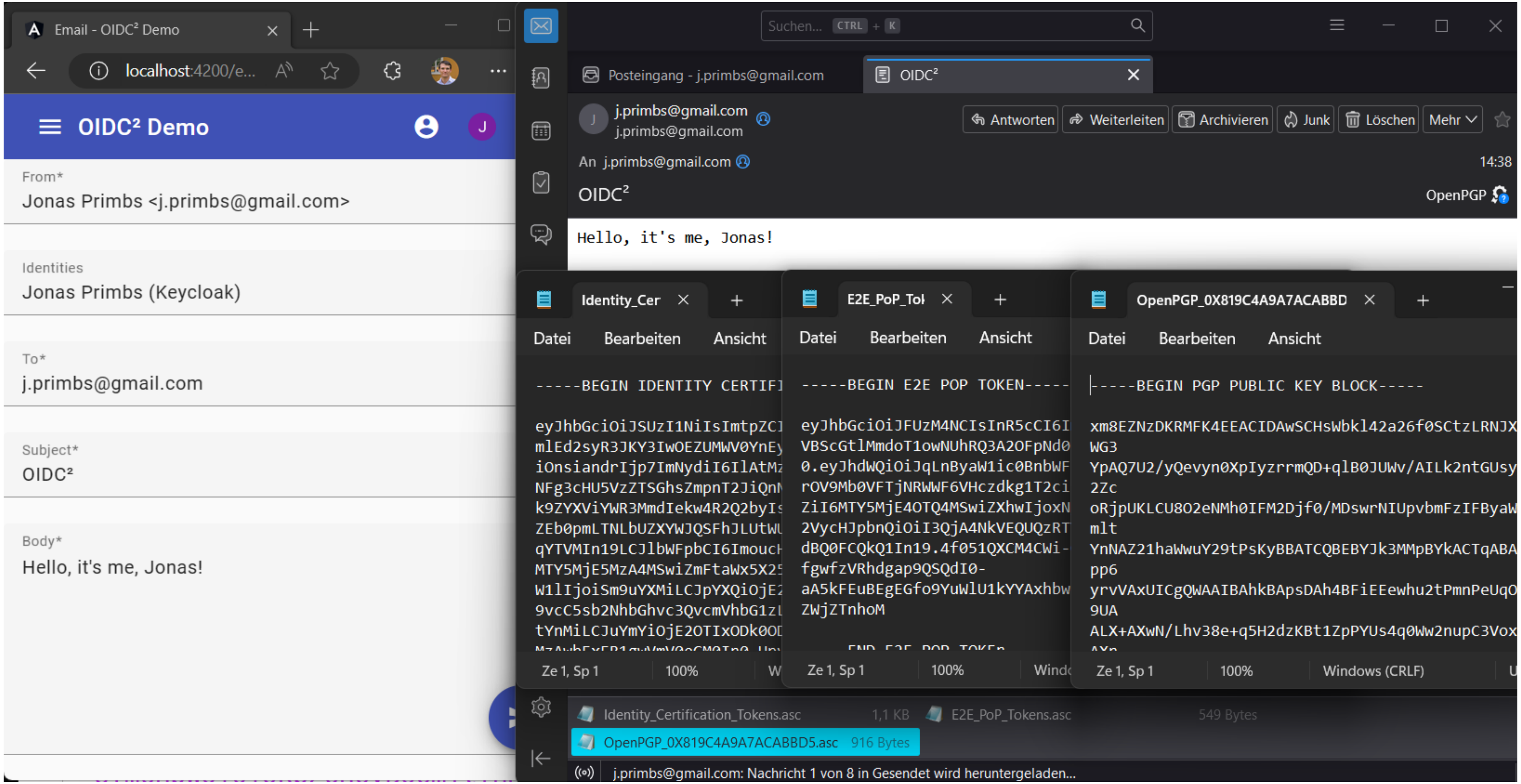
OpenID Provider (OP)
Identity Provider of the EU

Identity Certification Token (ICT)
JWT with identity claims of EU + public key of C (K_C^+), signed by OP, if proof of possession for K_C^- (PoP_C) is valid

Authenticating User (AU)
User who authenticates the EU

Authenticating Party (AP)
Client application of the AU

Prototype!



From*
Jonas Primbs <j.primbs@gmail.com>

Identities
Jonas Primbs (Keycloak)

To*
j.primbs@gmail.com

Subject*
OIDC²

Body*
Hello, it's me, Jonas!

j.primbs@gmail.com
j.primbs@gmail.com
An j.primbs@gmail.com
14:38
OIDC²

Hello, it's me, Jonas!

```
-----BEGIN IDENTITY CERTIFI

eyJhbGciOiJSUzI1NiIsImtpZCI
mlEd2syR3JKY3IwOEZUMWV0YnEy
iOnsiandrIjp7ImNydiI6IlAtMz
NFg3cHU5VzZTSGhsZmpnT2JiQnN
k9ZYXViYWR3MmdIekw4R2Q2byIs
ZEb0pmLTNLbUZXYWJQSFhJLUtWU
qYTVMIn19LCJlbWFpbCI6ImoucH
MTY5MjE5MzA4MSwiZmFtaWx5X25
W1lIjoiSm9uYXMiLCJpYXQiOjE2
9vcC5sb2NhbGhvc3QvcmVhbG1zL
tYnMiLCJuYmYiOjE2OTIxODk0OD
```

```
-----BEGIN E2E POP TOKEN-----

eyJhbGciOiJFUzM4NCIsInR5cCI6I
VBScGtlMmdoT1owNUhRQ3A2OFpNd0
0.eyJhdWQiOiJqLnByaW1ic0BnbWF
rOV9Mb0VFTjNRWWF6VHczdkg1T2ci
ZiI6MTY5MjE4OTQ4MSwiZXhwIjoxN
2VycHJpbnQiOiI3QjA4NkVEQUQzRT
dBQ0FCQkQ1In19.4f051QXCM4CWi-
fgwfzVRhdgap9QSQdI0-
aA5kFEuBEgEGfo9YuWlU1kYYAxhbw
ZWjZTnhoM
```

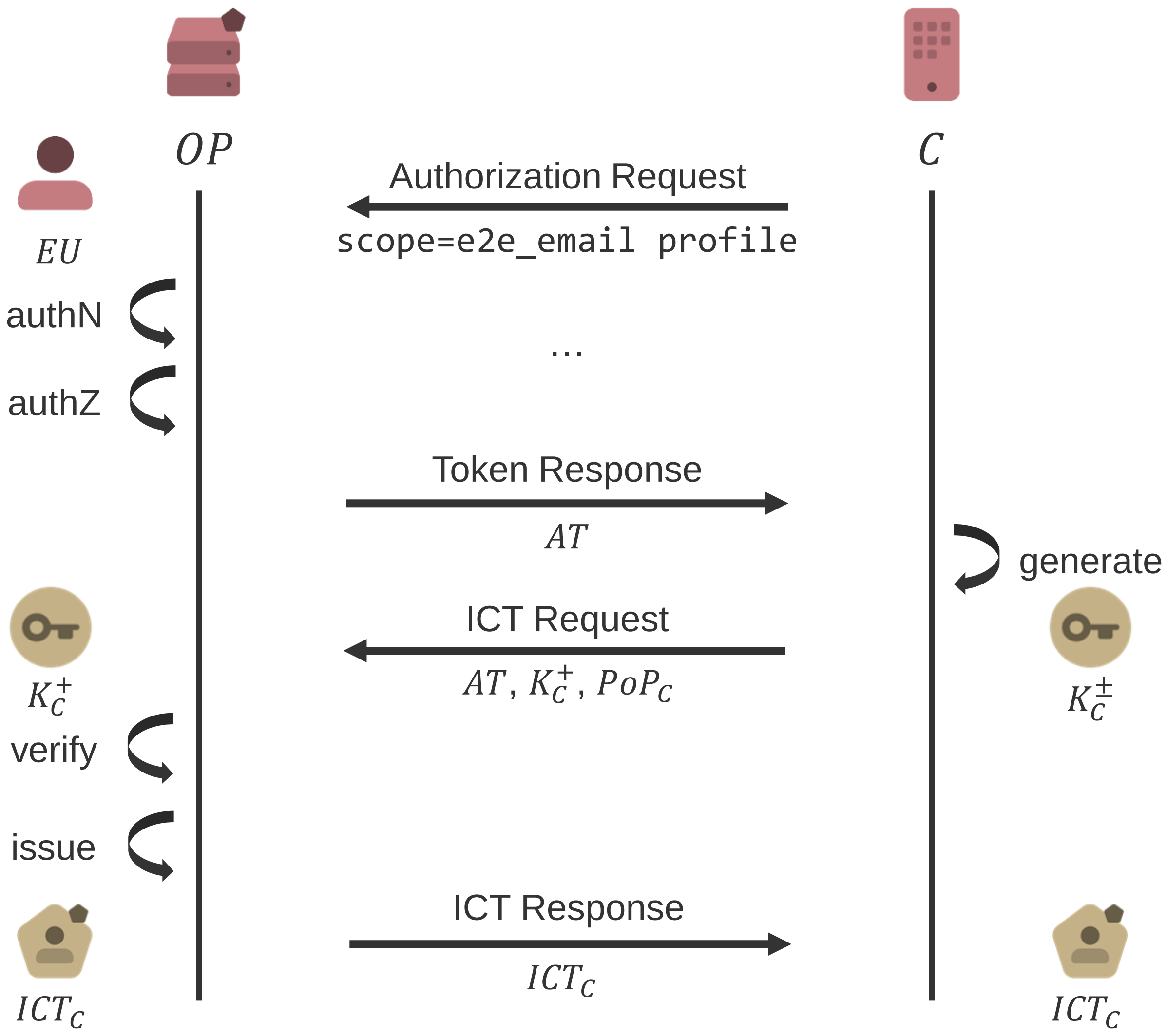
```
-----BEGIN PGP PUBLIC KEY BLOCK-----

xm8EZNzDKRMFK4EEACIDAwSCHsWbkl42a26f0SCtzLRNJX
WG3
YpAQ7U2/yQevyn0XpIyzrrmQD+qlB0JUWv/AILk2ntGUsy
2Zc
oRjpUKLCU8O2eNMh0IFM2Djf0/MDswrNIUpvbmFzIFByaW
mlt
YnNAZ21haWwuY29tPsKyBBATCQBEBYJk3MMpBYkACTqABA
pp6
yrvVAxUICgQWAAIBAhkBApsDAh4BFiEEwhu2tPmnPeUqO
9UA
ALX+AXwN/Lhv38e+q5H2dzKBt1ZpPYUs4q0Ww2nupC3Vox
```

Identity_Certification_Tokens.asc 1,1 KB
E2E_PoP_Tokens.asc 549 Bytes
OpenPGP_0X819C4A9A7ACABBD5.asc 916 Bytes

j.primbs@gmail.com: Nachricht 1 von 8 in Gesendet wird heruntergeladen...

Recap + Update: Obtain an ICT

1. C sends OAuth 2 Authorization Request to OP
   - Contains scope request for end-to-end context (`e2e_email`) and profile information (`profile`)
2. EU authenticates to OP and authorizes requested scopes
3. OP responds with Access Token (AT) in Token Response
   - AT authorizes for granted scopes
4. C generates asymmetric key pair $K_C^{\pm}$
5. C sends ICT Request to OP
   - Contains public key AT, K_C^+, and PoP of K_C^-
6. OP verifies ICT Request
   - Requires verification of AT and PoP
7. RP issues ICT in ICT Response

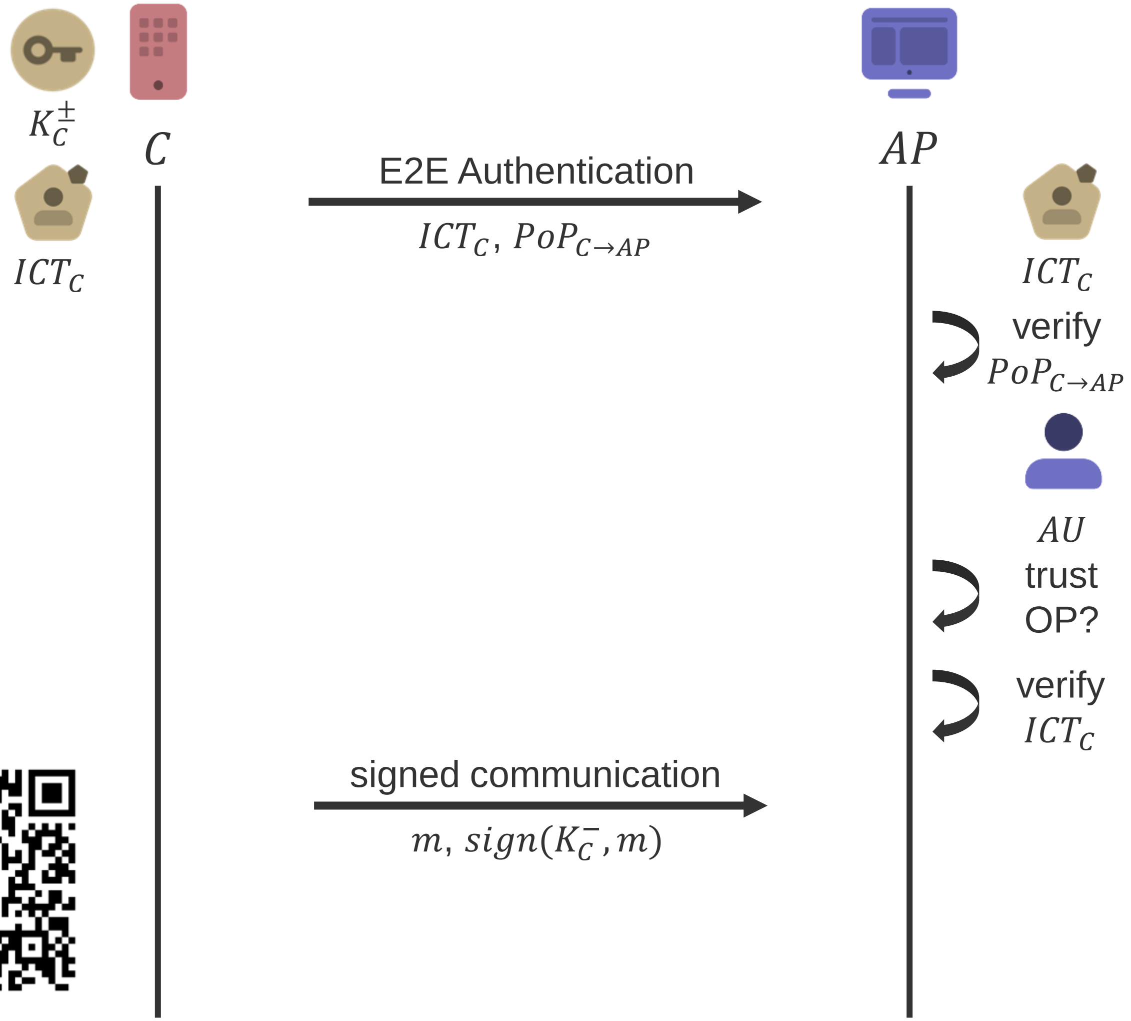


Recap + Update: Use an ICT

1. C sends E2E Authentication message to AP
   - Contains ICT and a new PoP for the AP
2. AP verifies ICT and PoP
   - PoP valid for ICT's K_C^+?
   - Does the AU trust the OP?
   - ICT valid?

- ► Continue with signed communication
  - Using trusted K_C^- as signing key
- ► We call it "**Open Identity Certification for OIDC**"
  - Aka **OIDC²**
- ► Draft is on GitHub!
  - Pull requests and discussions are welcome!

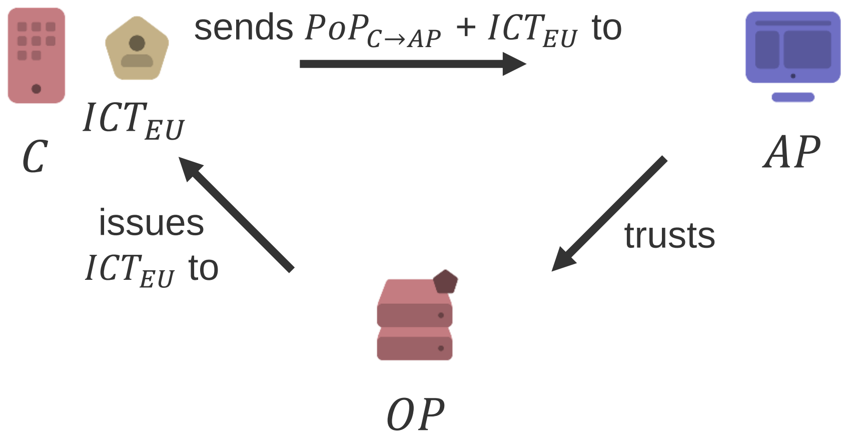
https://bit.ly/oidc2



OIDC^2 vs. SSI

OIDC^2

- Trust relationship:



sends $PoP_{C \to AP}$ + ICT_{EU} to

C

ICT_{EU}

AP

issues ICT_{EU} to

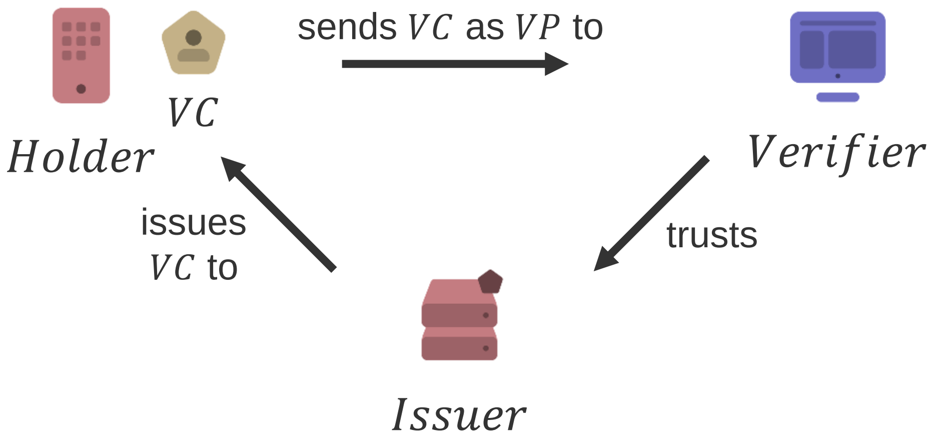
trusts

OP

- ICT attests identity claims of EU
- C authenticates with PoP + ICT to AP
- Requires deployed OIDC infrastructure
- Key pair and ICT are **short-lived**
- **No** key revocation mechanism required

SSI

- Trust relationship:



sends VC as VP to

$Holder$

VC

$Verifier$

issues VC to

trusts

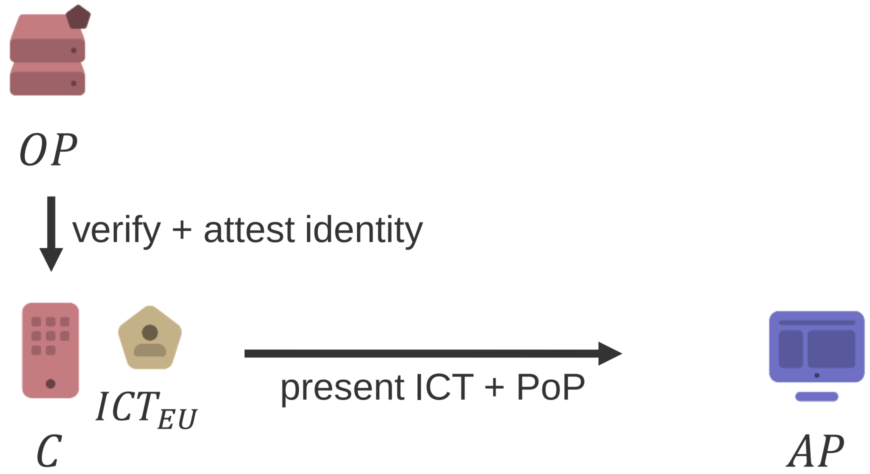
$Issuer$

- VC attests claims of Holder
- Holder authenticates with VP to Verifier
- Requires deployed SSI infrastructure
- Key pair and VC are **long-lived**
- Key revocation requires verification

OIDC² vs. PKI

OIDC²

- Trust relationship:



OP

verify + attest identity

C ICT_{EU}

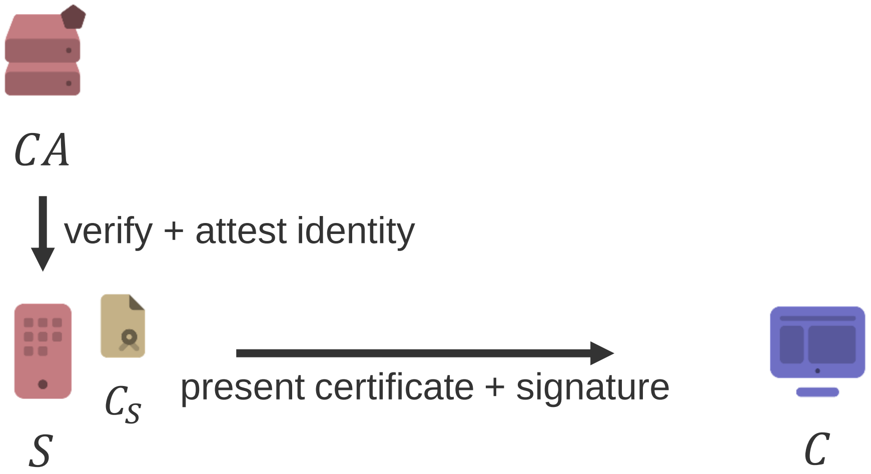
present ICT + PoP

AP

- AP must trust OP
- EU signs into OP; C proves possession of K_C^- to obtain an ICT
- AP authenticates C by ICT and PoP
- **No** key revocation mechanism required

PKI

- Trust relationship:



CA

verify + attest identity

S C_S

present certificate + signature

C

- Client (C) must trust Certificate Authority (CA)
- Service (S) performs ACME challenge to obtain an X.509 certificate
- C authenticates S by certificate and signature
- Key revocation requires verification

When (not) to use OIDC^2?

Do!

- Users authenticate themselves end-to-end
  - Intermediate services are not trusted
- Users identify each other with OIDC accounts
  - Or claims the OP is an authority for
- Users authenticate themselves only online
  - ICTs are requested on demand

Don’t!

- Users authenticate to intermediate services
  - Use normal OIDC instead
- Users identify each other via attributes
  - Requires attestation by authority (CA or Issuer)
- Users may authenticate themselves offline
  - Requires long-lived certificates or VCs

Outlook

- Next steps:
  - Prototype for instant messaging with Matrix
  - Prototype for video conferencing with WebRTC
  - Further improve OpenID Draft

https://bit.ly/oidc2

- Suggestions welcome!
  - Feel free to open discussions on GitHub
- Participation welcome!
  - Feel free to send a pull request on GitHub

- Want to stay in touch?
  - Here are my OIDC profiles:

    in /in/jonasprimbs

    X /JonasPrimbs

  - Or mail to: jonas.primbs@uni-tuebingen.de

Thank you!