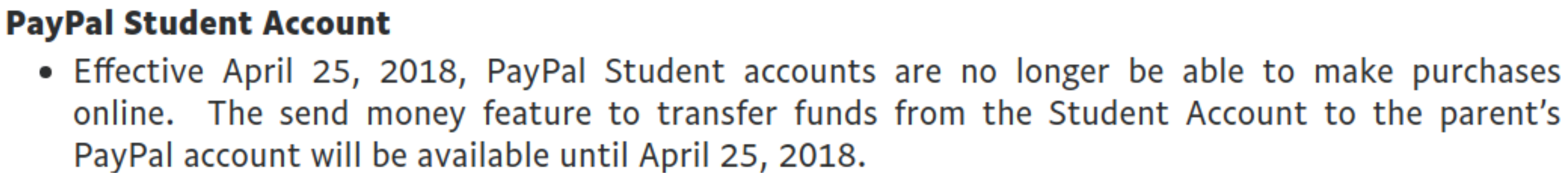
DelegaTEE: Brokered Delegation using Trusted Execution Environments

Sinisa Matetic (ETH Zurich), Moritz Schneider (ETH Zurich), Andrew Miller (UIUC), Ari Juels (Cornell Tech), Srdjan Capkun (ETH Zurich)

27th Usenix Security Symposium, August 12-17, 2018, Baltimore, MD, USA

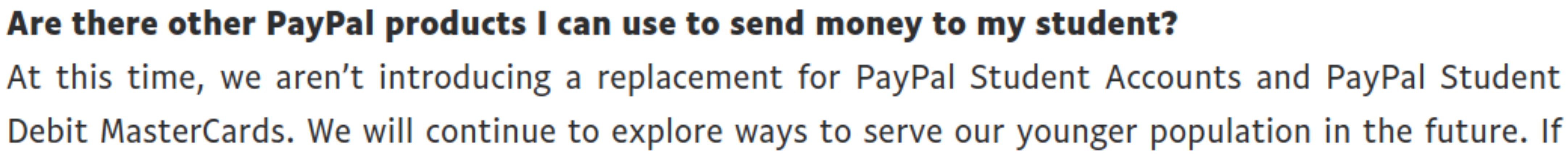
Motivation – Account sharing with restrictions

Motivation – Account sharing with restrictions



PayPal Student Account

- Effective April 25, 2018, PayPal Student accounts are no longer be able to make purchases online. The send money feature to transfer funds from the Student Account to the parent's PayPal account will be available until April 25, 2018.



Are there other PayPal products I can use to send money to my student?

At this time, we aren't introducing a replacement for PayPal Student Accounts and PayPal Student Debit MasterCards. We will continue to explore ways to serve our younger population in the future. If

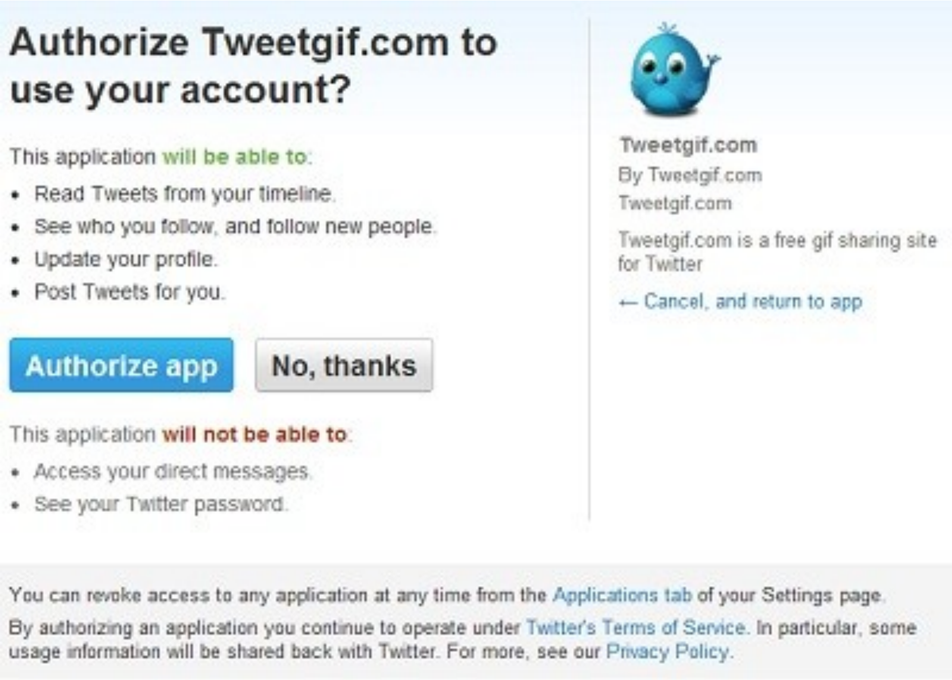
Motivation – Account sharing with restrictions

- Bob really wants to make Alice happy…
- Bob is fine sharing his account…
- But, he doesn't really want to reveal his login credentials to Alice and also give her unlimited spending capabilities…

- (since Bob is very security aware and uses the same password in all web service that he has… :D)

Motivation – Account sharing with restrictions

- If only the service would support such a scheme…
- Applicable to all types of online services and action performed on the web
  - Delegation is only possible if directly supported by the service provider



Authorize Tweetgif.com to use your account?

This application will be able to:

- Read Tweets from your timeline.
- See who you follow, and follow new people.
- Update your profile.
- Post Tweets for you.

This application will not be able to:

- Access your direct messages.
- See your Twitter password.

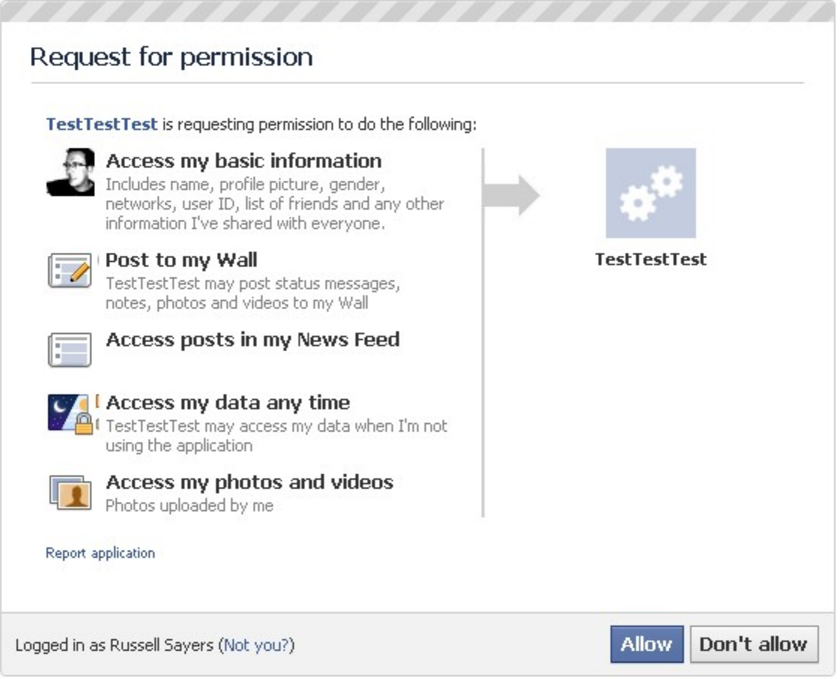
Tweetgif.com
By Tweetgif.com
Tweetgif.com

Tweetgif.com is a free gif sharing site for Twitter

← Cancel, and return to app

You can revoke access to any application at any time from the Applications tab of your Settings page.

By authorizing an application you continue to operate under Twitter's Terms of Service. In particular, some usage information will be shared back with Twitter. For more, see our Privacy Policy.



Request for permission

TestTestTest is requesting permission to do the following:

Access my basic information
Includes name, profile picture, gender, networks, user ID, list of friends and any other information I've shared with everyone.

Post to my Wall
TestTestTest may post status messages, notes, photos and videos to my Wall

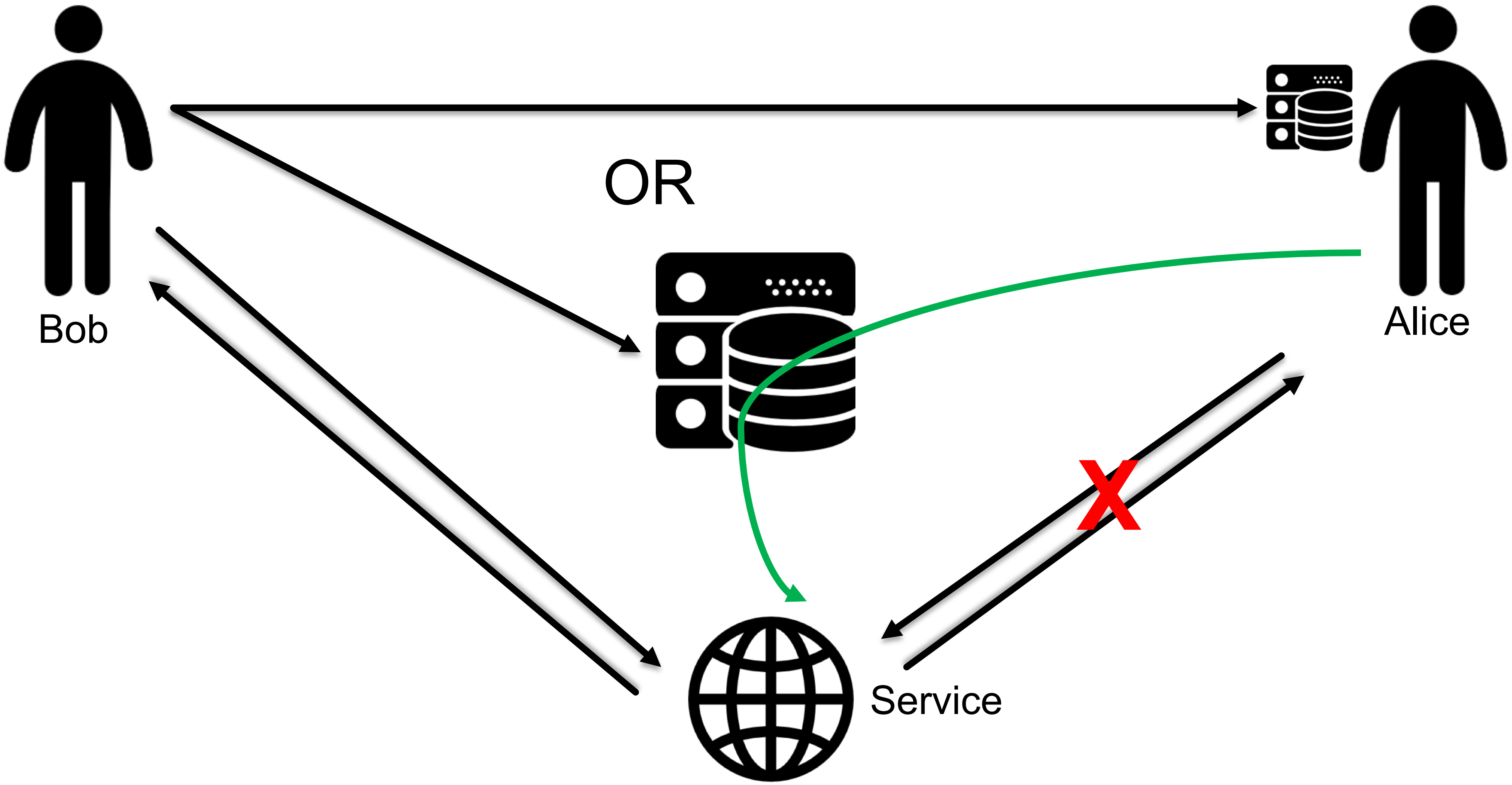
Access posts in my News Feed

Access my data any time
TestTestTest may access my data when I'm not using the application

Access my photos and videos
Photos uploaded by me

Logged in as Russell Sayers (Not you?)

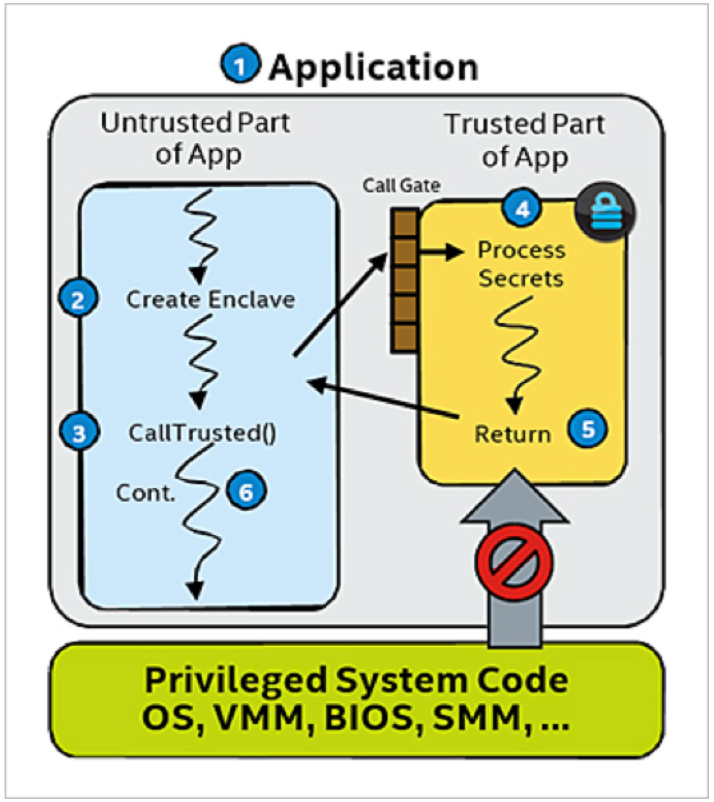
Solution – Brokered Delegation



- DelegaTEE: Brokered Delegation using Trusted Execution Environments

Trusted Execution Environments

- Enable isolated execution within a user’s system
  - ARM Trustzone, Intel SGX, …
- Intel SGX – secure enclaves
  - Runtime isolation, ecall/ocall interfaces, sealing, attestation
  - Memory content encrypted



- NOTE: Recent work shows successful compromise of such environments
  - Side-channel attacks, Spectre, Meltdown, Foreshadow (see talks from yesterday)
  - Patches on the way

Images taken from software.intel.com

Our contribution: Brokered Delegation with enclaves

- A new concept that seems very familiar
- Flexibly, securely and selectively share and delegate access (credentials and rights)
- No explicit support (or even knowledge) of the service providers
- Fine-grained delegation without trust between the credential owner and other users
- Supported with the usage of TEEs
- Credential Owners (give access) and Delegatees (receive restricted access)

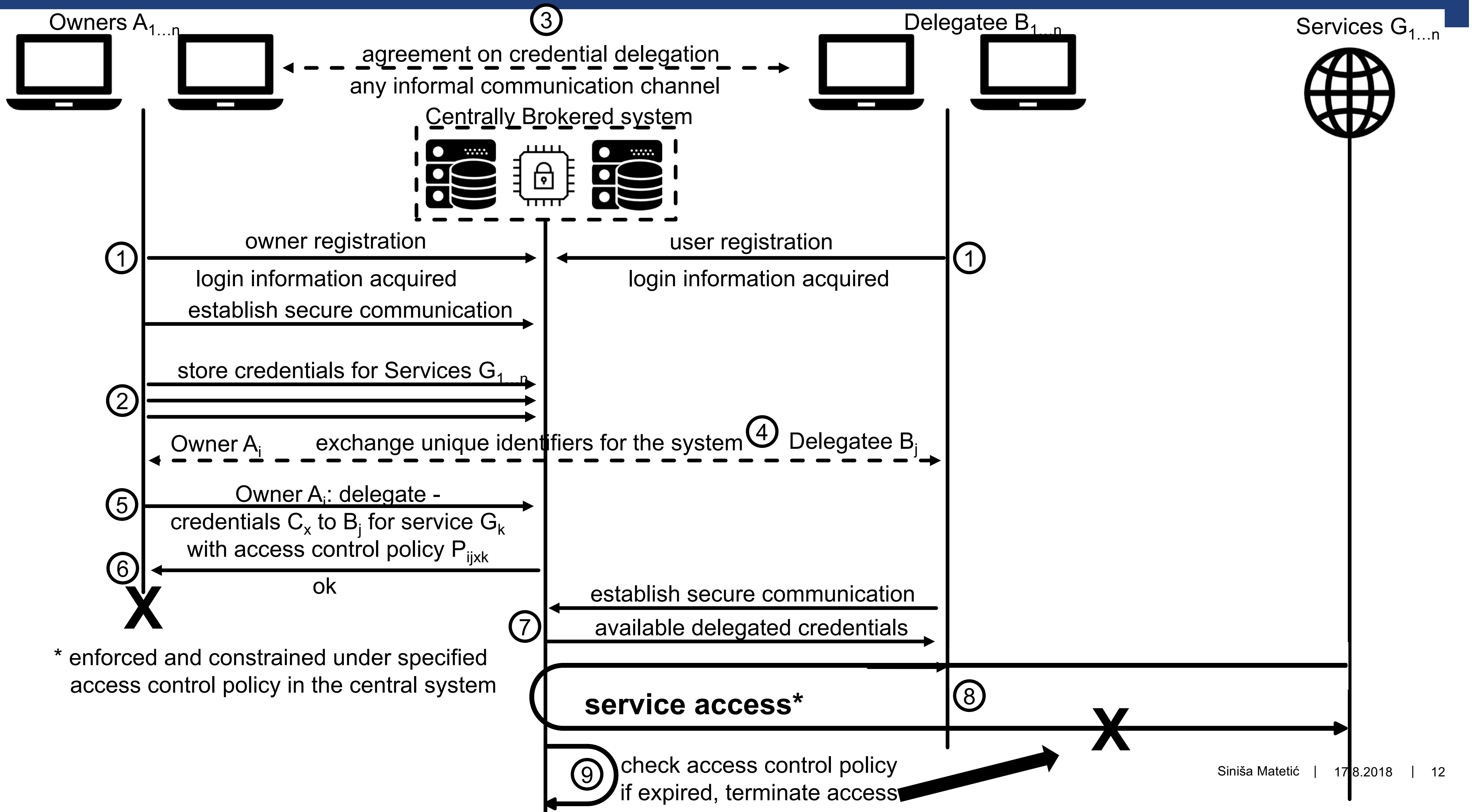
DelegaTEE - Challenges and desired properties

- The Owner’s credentials remain confidential.
- The Owner can restrict access to his account, e.g., in terms of time, duration of access, no. of reads/writes etc. - with rich contextual policies
- The system logs the actions of Owners and Delegatees so that post-hoc attribution of their behaviour is possible (as a means of resolving disputes)
- The system minimizes the ability of a service to distinguish between access by the Delegatee and that of the legitimate Owner

- Owner does not have to always be online

DelegaTEE – two system designs

- Peer-to-peer system model
- Centrally brokered system model



Owners $A_{1...n}$

Delegatee $B_{1...n}$

Services $G_{1...n}$

3 agreement on credential delegation

any informal communication channel

Centrally Brokered system

1 owner registration

login information acquired

establish secure communication

user registration 1

login information acquired

2 store credentials for Services $G_{1...n}$

Owner A_i exchange unique identifiers for the system 4 Delegatee B_j

5 Owner A_i: delegate -

credentials C_x to B_j for service G_k

with access control policy P_{ijxk}

6 ok

X

establish secure communication

7 available delegated credentials

* enforced and constrained under specified access control policy in the central system

service access* 8

X

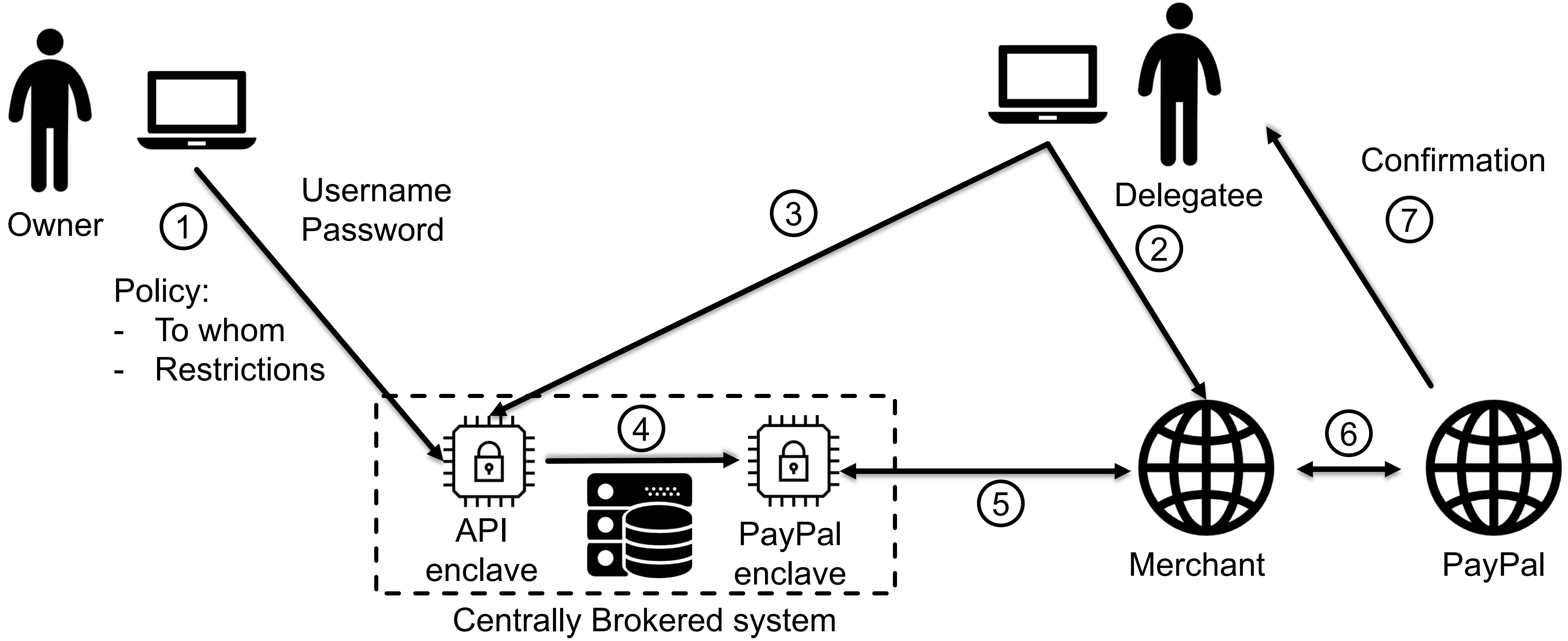
9 check access control policy

if expired, terminate access

Trust assumptions and security

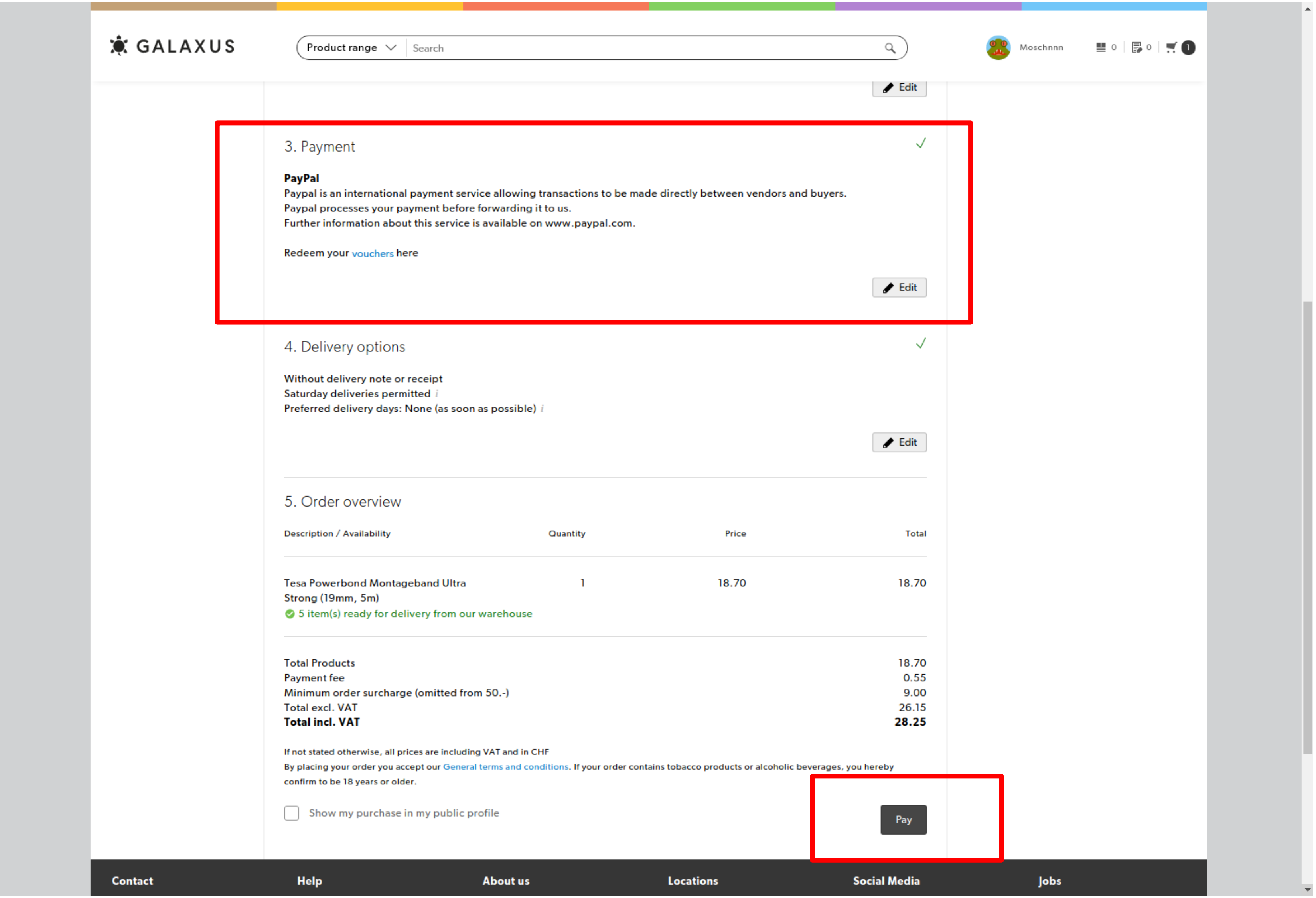
- Intel SGX enclaves are trusted for confidentiality and attestation
  - The Owner is to be fully protected
- Server and the operator *per se* do not need to be trusted
- System works as trusted a proxy, a man-in-the-middle
  - End-to-end TLS from enclave-to-delegatee and enclave-to-service

Case Study Implementation 1: PayPal



ETH zürich

Demo



3. Payment ✓

PayPal
Paypal is an international payment service allowing transactions to be made directly between vendors and buyers.
Paypal processes your payment before forwarding it to us.
Further information about this service is available on www.paypal.com.

Redeem your vouchers here

4. Delivery options ✓

Without delivery note or receipt
Saturday deliveries permitted
Preferred delivery days: None (as soon as possible)

5. Order overview

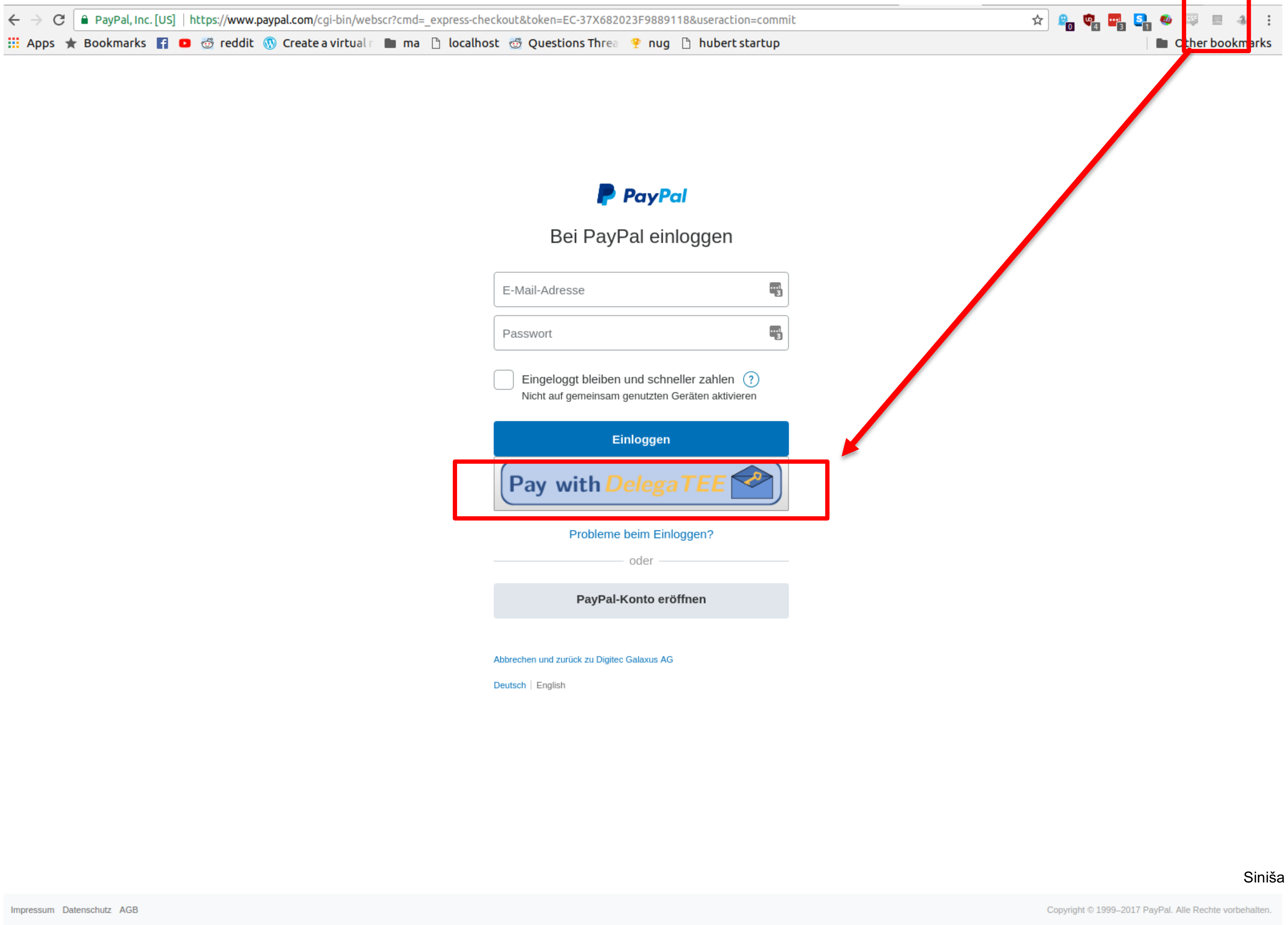
Description / Availability	Quantity	Price	Total
Tesa Powerbond Montageband Ultra Strong (19mm, 5m) 5 item(s) ready for delivery from our warehouse	1	18.70	18.70

Total Products	18.70
Payment fee	0.55
Minimum order surcharge (omitted from 50.-)	9.00
Total excl. VAT	26.15
Total incl. VAT	**28.25**

If not stated otherwise, all prices are including VAT and in CHF
By placing your order you accept our General terms and conditions. If your order contains tobacco products or alcoholic beverages, you hereby confirm to be 18 years or older.

□ Show my purchase in my public profile

Demo



PayPal, Inc. [US] | https://www.paypal.com/cgi-bin/webscr?cmd=_express-checkout&token=EC-37X682023F9889118&useraction=commit

PayPal

Bei PayPal einloggen

E-Mail-Adresse

Passwort

□ Eingeloggt bleiben und schneller zahlen ?
Nicht auf gemeinsam genutzten Geräten aktivieren

Einloggen

Pay with DelegaTEE

Probleme beim Einloggen?

oder

PayPal-Konto eröffnen

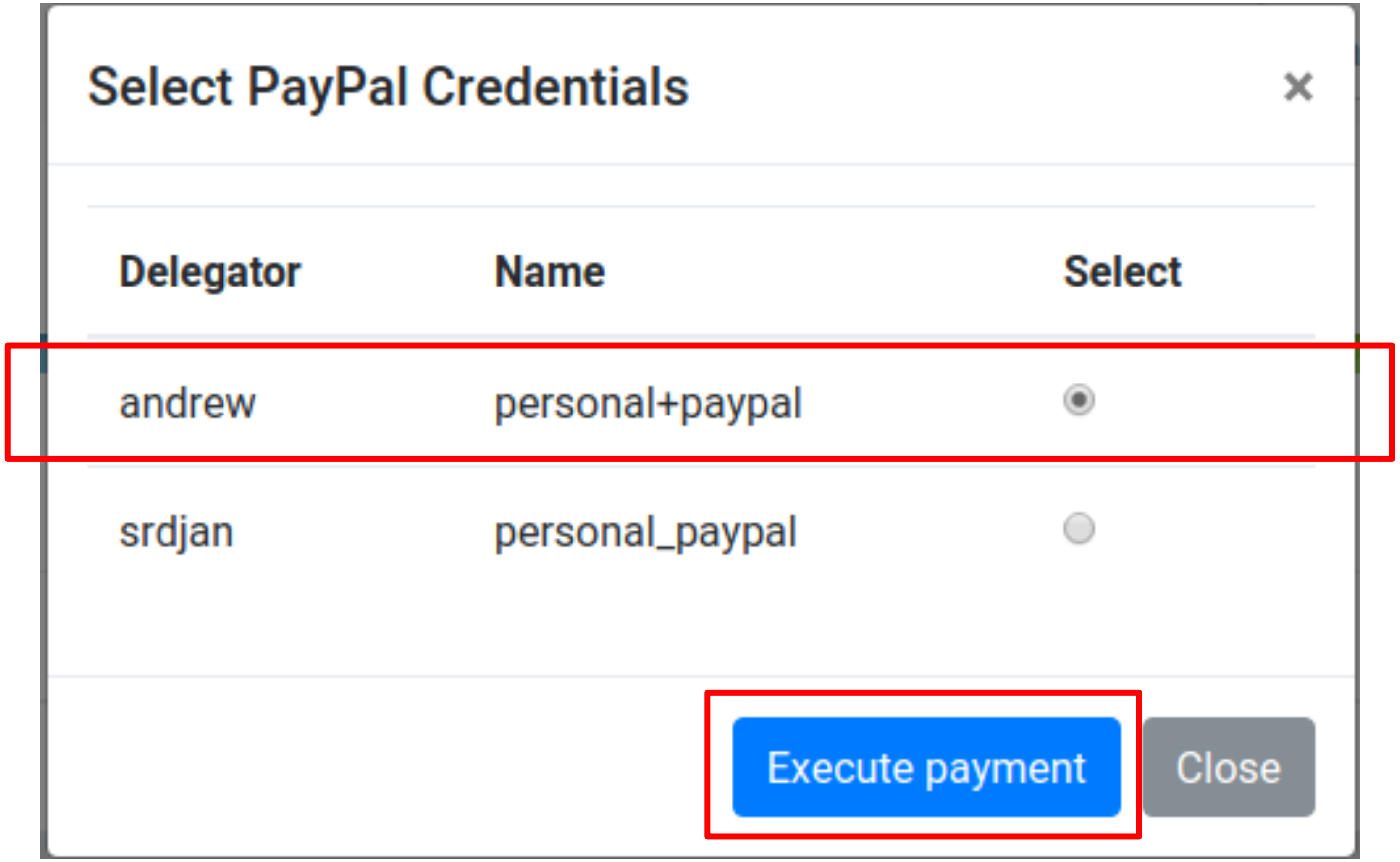
Abbrechen und zurück zu Digitec Galaxus AG

Deutsch | English

Impressum Datenschutz AGB

Copyright © 1999–2017 PayPal. Alle Rechte vorbehalten.

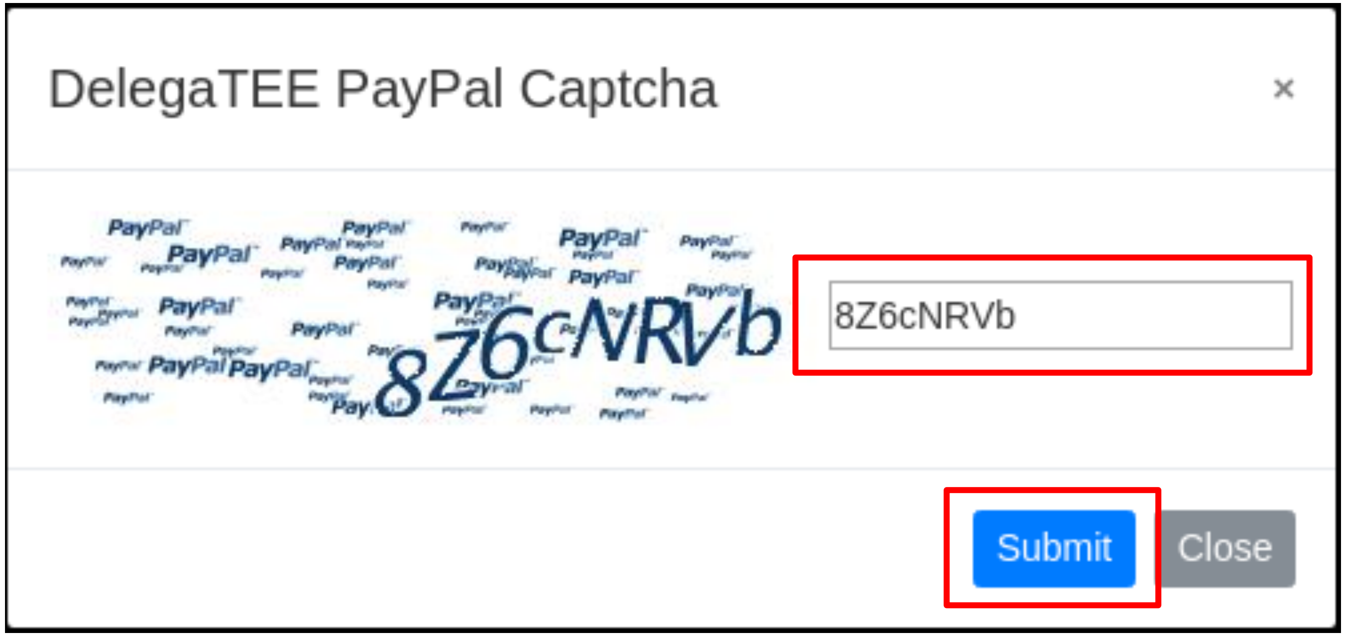
Demo



Select PayPal Credentials

Delegator	Name	Select
andrew	personal+paypal	●
srdjan	personal_paypal	○

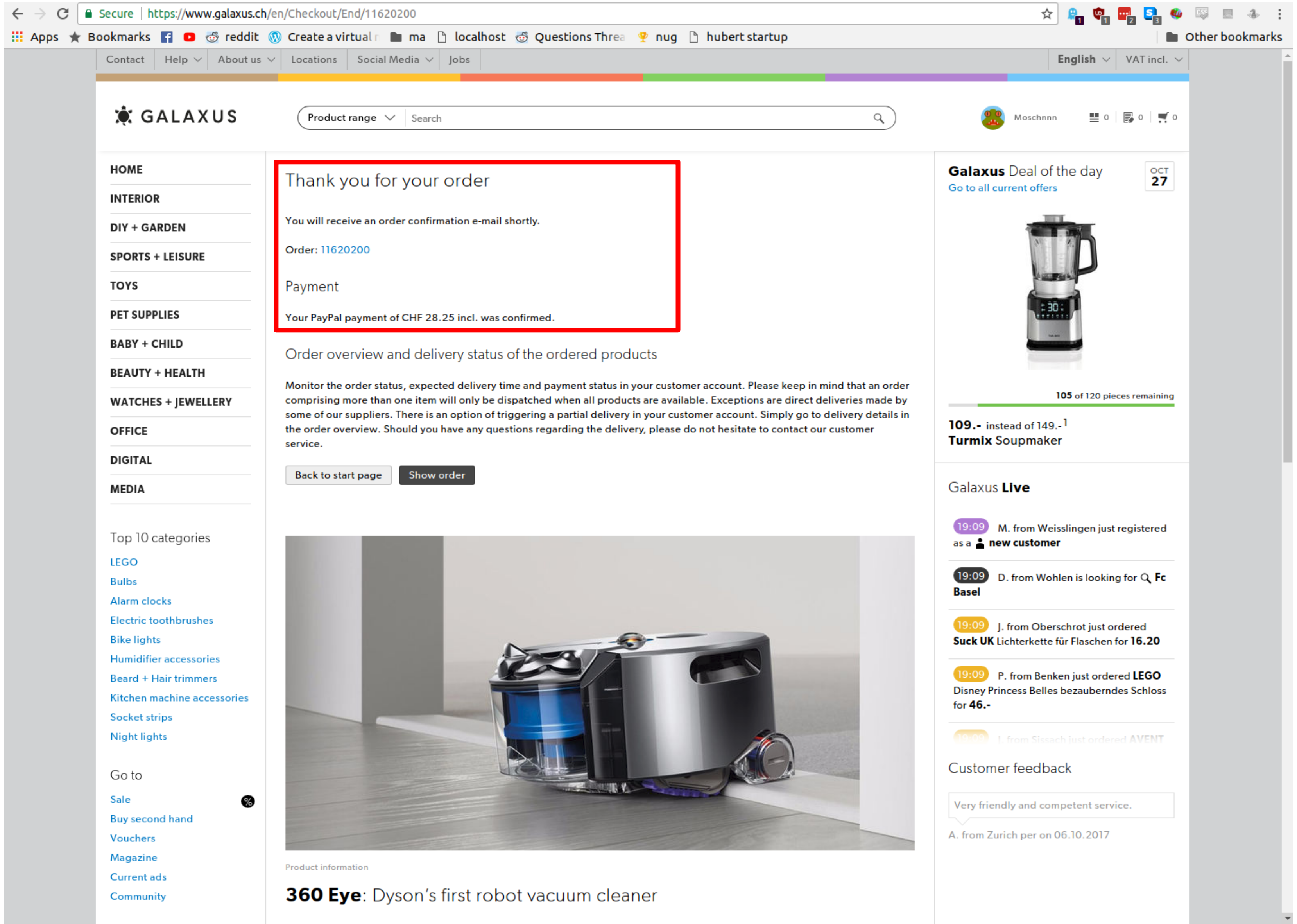
Demo



DelegaTEE PayPal Captcha

8Z6cNRVb

Demo



Thank you for your order

You will receive an order confirmation e-mail shortly.

Order: 11620200

Payment

Your PayPal payment of CHF 28.25 incl. was confirmed.

Order overview and delivery status of the ordered products

Monitor the order status, expected delivery time and payment status in your customer account. Please keep in mind that an order comprising more than one item will only be dispatched when all products are available. Exceptions are direct deliveries made by some of our suppliers. There is an option of triggering a partial delivery in your customer account. Simply go to delivery details in the order overview. Should you have any questions regarding the delivery, please do not hesitate to contact our customer service.

Product information

360 Eye: Dyson's first robot vacuum cleaner

Galaxus Deal of the day

OCT 27

Go to all current offers

105 of 120 pieces remaining

109.- instead of 149.-[1]

Turmix Soupmaker

Galaxus **Live**

19:09 M. from Weisslingen just registered as a **new customer**

19:09 D. from Wohlen is looking for **Fc Basel**

19:09 J. from Oberschrot just ordered **Suck UK** Lichterkette für Flaschen for **16.20**

19:09 P. from Benken just ordered **LEGO** Disney Princess Belles bezauberndes Schloss for **46.-**

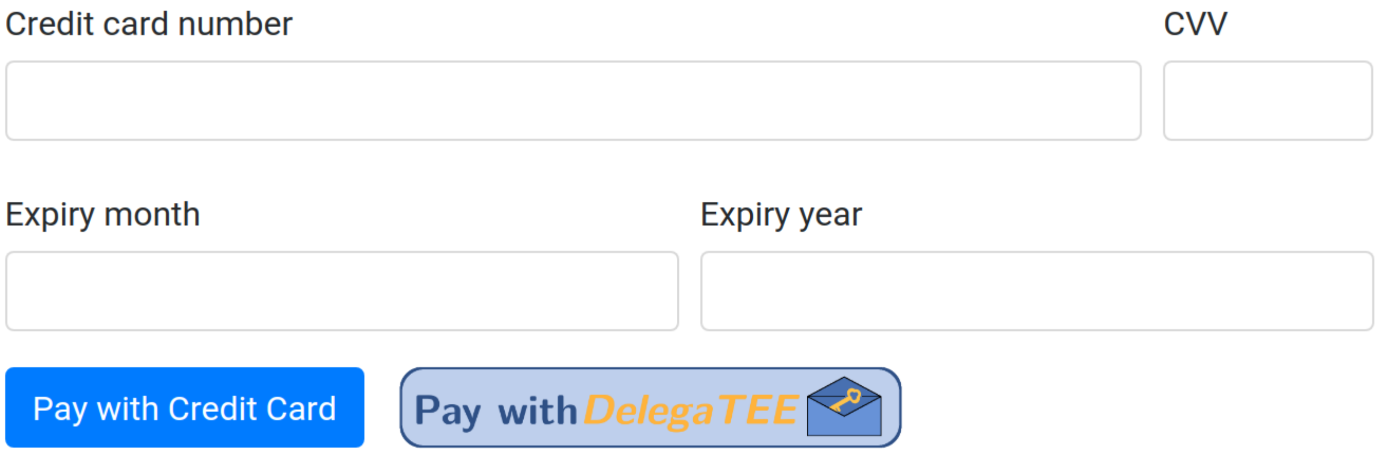
19:09 J. from Sissach just ordered **AVENT**

Customer feedback

Very friendly and competent service.

A. from Zurich per on 06.10.2017

Case Study Implementation 2: Credit Card - Demo

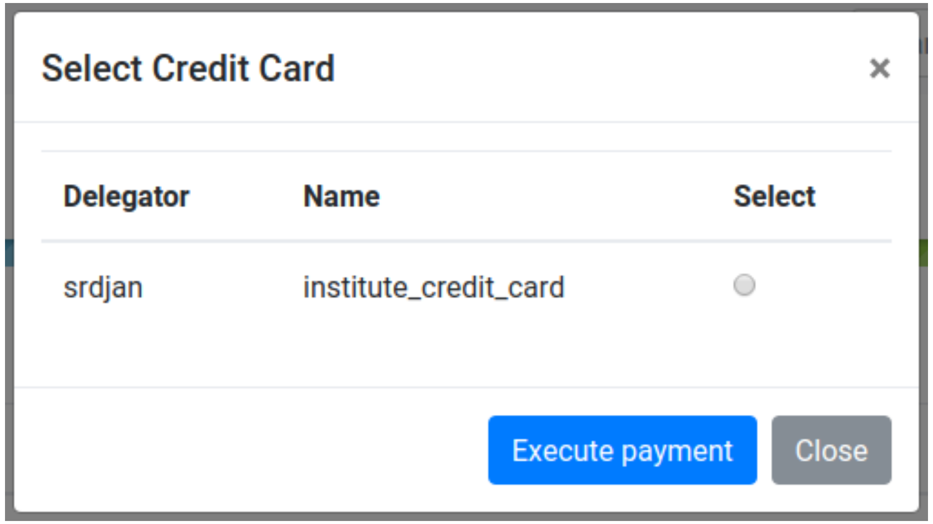


Credit card number

CVV

Expiry month

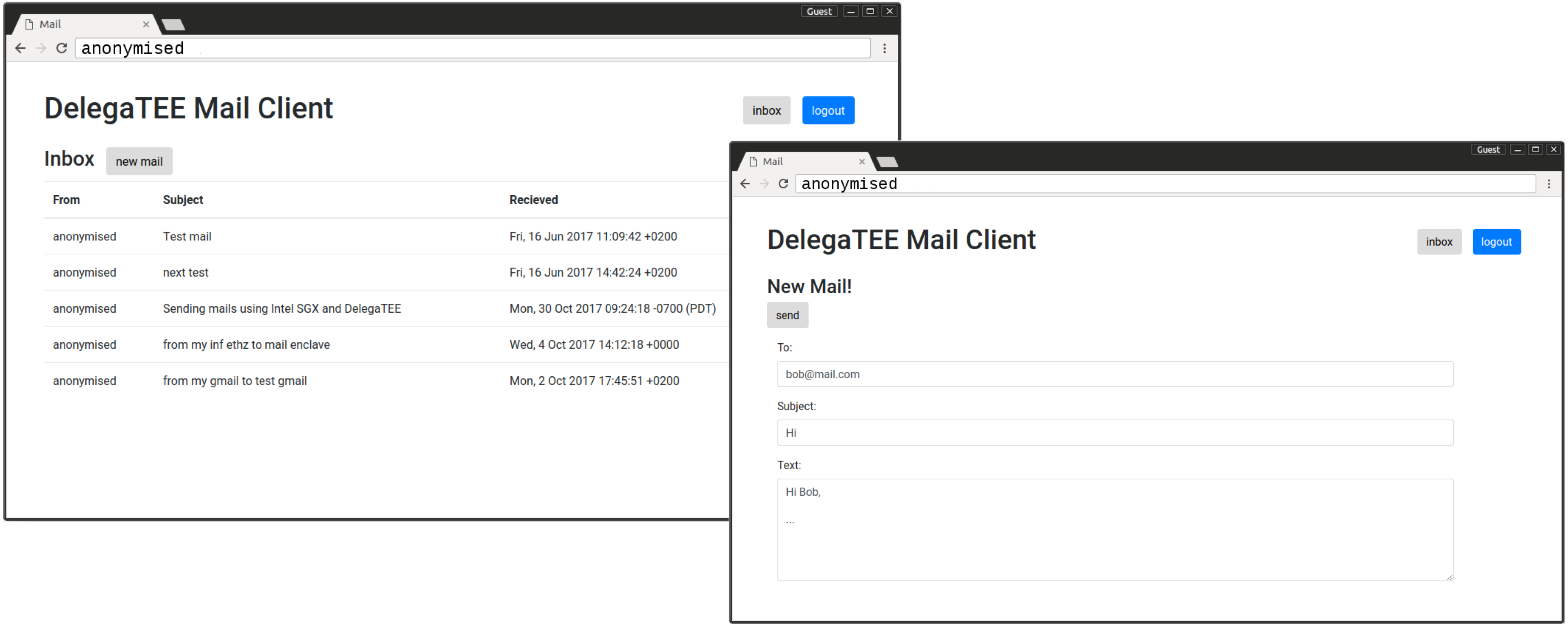
Expiry year



Select Credit Card

Delegator	Name	Select
srdjan	institute_credit_card	○

Case Study Implementation 3: Email - Demo



DelegaTEE Mail Client

Inbox

From	Subject	Recieved
anonymised	Test mail	Fri, 16 Jun 2017 11:09:42 +0200
anonymised	next test	Fri, 16 Jun 2017 14:42:24 +0200
anonymised	Sending mails using Intel SGX and DelegaTEE	Mon, 30 Oct 2017 09:24:18 -0700 (PDT)
anonymised	from my inf ethz to mail enclave	Wed, 4 Oct 2017 14:12:18 +0000
anonymised	from my gmail to test gmail	Mon, 2 Oct 2017 17:45:51 +0200

DelegaTEE Mail Client

New Mail!

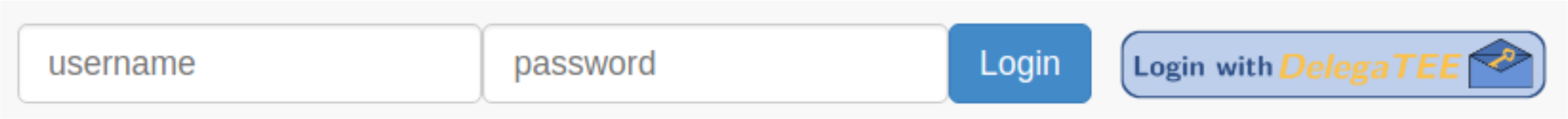
To:
bob@mail.com

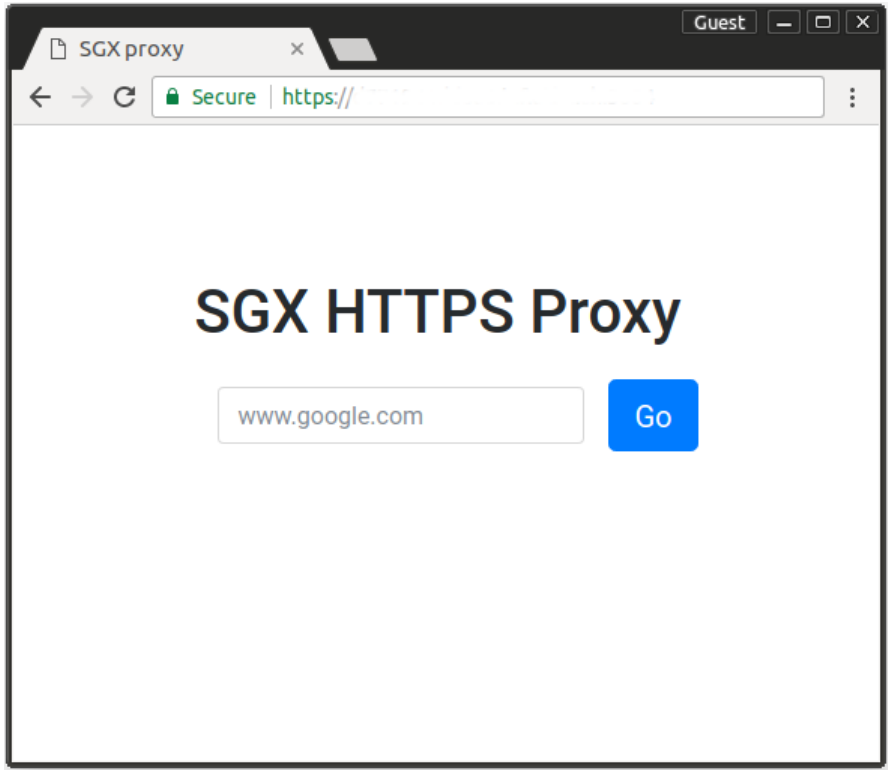
Subject:
Hi

Text:
Hi Bob,

...

Case Study Implementation 4: General website browsing - Demo





SGX HTTPS Proxy

Performance

- In line with the original performance of the use case scenario
- P2P system
  - Minimal and negligible overhead
  - Functions as a local proxy
  - Supports all provided use-cases
- Centrally Brokered System
  - Serves all delegation request through a central system
  - All use cases except video streaming handled almost instantaneously
  - No. of concurrent users depends on the server hardware

Brokered Delegation may undermine service’s policy enforcement

- MAC-to-DAC
  - Similar to the `setuid` in Unix systems
- Building secondary markets for any service
  - Netflix, and any other video streaming service
  - Paid subscription services, such as news portals, etc.
  - …
- Services expect the difficulty of broadly sharing credentials

Discussion, Challenges and Limitations

- Identity-based model
- Anonymous model

- Policy creation and enforcement
  - Easy for standardized protocols and messages
  - More difficult for a general use-case example
  - Curated ”policy app store” for different use cases?

For more details please see the paper!

Discussion, Challenges and Limitations

- Authentication challenges
  - Two-step authentication
  - CAPTCHA
- Authentication Collisions
- Usability
- Deployment
- Service Prevention
- Scalability

For more details please see the paper!

Summary & Conclusion

- Secure and flexible delegation of user access rights and credentials
- Applicable for online transactions with password-based authentication
  - Can be developed to support brick-and-mortar transactions
- No changes needed on the service side
- Compatibility with wide range of services
- Rise of new sharing economies and business models
- A potential game changer? Market disruptor?

Thank you for your attention! Questions?

Sinisa Matetic

ETH Zurich
System Security Group
Institute of Information Security
Department of Computer Science

www.syssec.ethz.ch

sinisa.matetic@inf.ethz.ch