

PARADISE

**Privacy-enhancing And Reliable Anti-Doping
Integrated Service Environment**

Dr. Denis Giffeler and Sebastian Zickau

GeoIT WhereCamp Conference 2017 | 30.11.2017



**WORLD
ANTI-DOPING
AGENCY**
play true

**ALLES
GEBEN,
NICHTS
NEHMEN.**

nada
FÜR SAUBERE LEISTUNG

Wada

Fancy Bears hack again with attack on senior anti-doping officials

- Email content includes blood values of US athletes
- Contains personal details of Wada's Sir Craig Reedie



This article is 12 months old

118

Sean Ingle

@seaningle

Friday 25 November 2016 22.20 GMT



Emails hacked from Wada include conversations about high-profile US athletes who might have unusual blood values and strong suggestions that an athlete, who has not been banned, had a blood transfusion before a major race. Photograph: Marc Braibant/AFP/Getty Images

The cyber-espionage group Fancy Bears, which made headlines worldwide when it published the private medical certificates of athletes including Bradley Wiggins, Serena Williams and Simone Biles, has struck again by hacking into the confidential emails of senior anti-doping officials.

Most popular



Japan anger over South Korea's shrimp surprise for Donald Trump



Louis CK: laughter ends as years of allegations dog comedy star



Nuclear accident in Russia or Kazakhstan sends 'harmless' radioactive cloud over Europe



Canada's naked car crash takes new twist as three face kidnapping charges

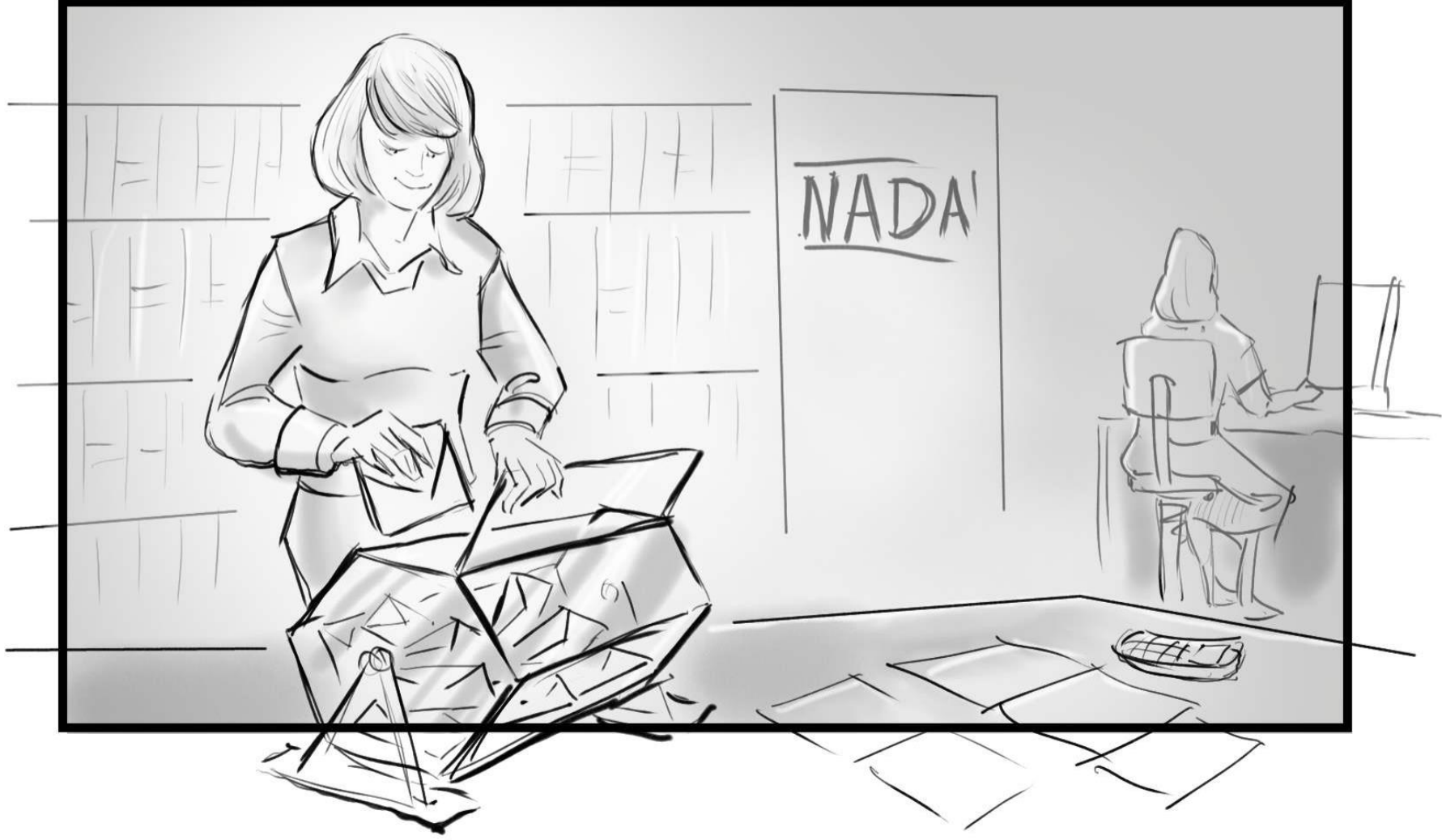


Chinese media hails success of Trump's 'pilgrimage' to Beijing









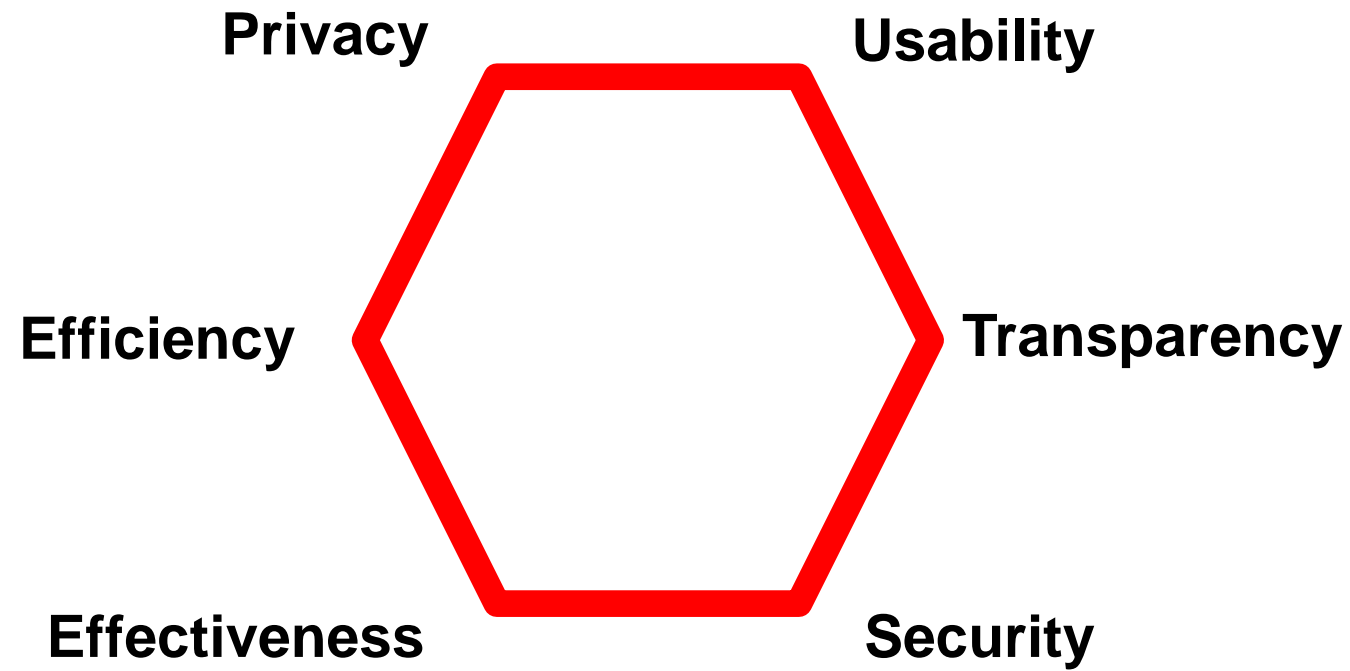




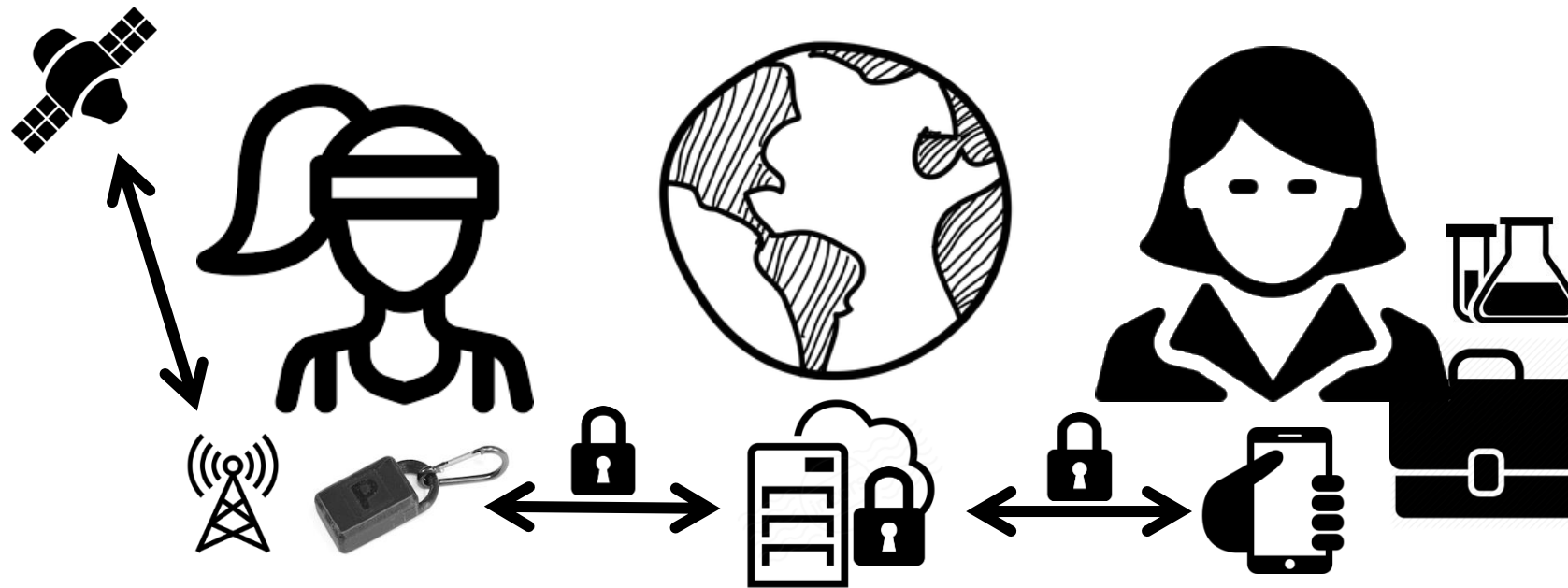


- First ideas for localization-based Anti-Doping System EVES were developed in early 2012 by 400m runner Jonas Plass
- Starting 2013 Mr. Plass and Dr. Denis Giffeler (gekko mbH) devised a fully detailed concept, which then materialized into PARADISE
- Fraunhofer AISEC & FIT, Technische Universität Berlin, ULD, Uniscon and gekko are partners in this government-funded research project

- WADA | NADO | NADA
- ADAMS (Anti-Doping Administration & Management System)
- Whereabouts
- Doping Control Officer (DCO)
- eves-device
- ADAMS → eves → PARADISE
- Missed tests → strikes → 3 strikes = positive test
- 1 hour time window for top tier athletes
- Test usually conducted between 6:00am – 11:00pm (example wedding/birthday)



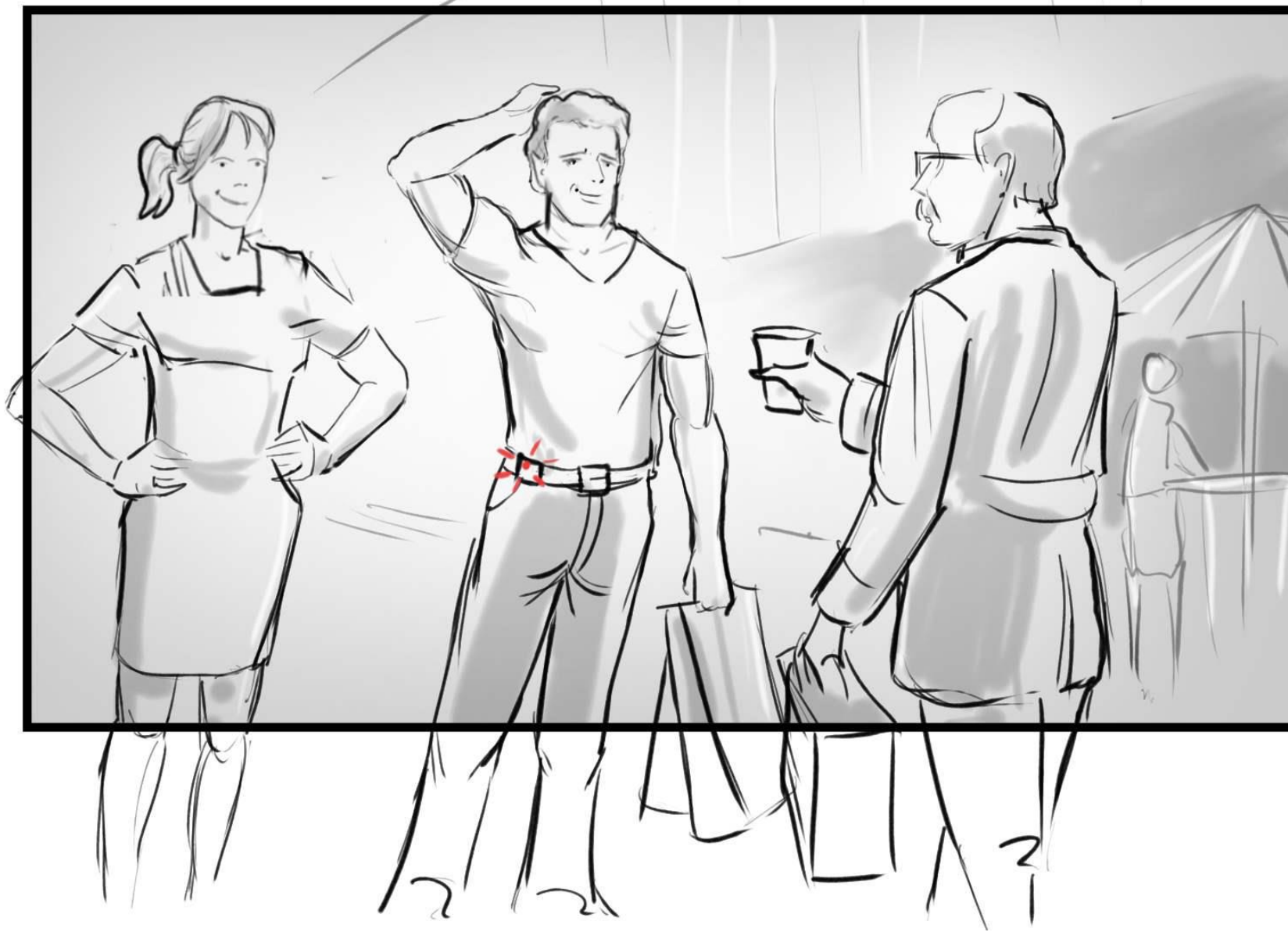
A new approach



- Using location-based eaves-devices (reactively)
- Minimizing data collection
- Providing more accurate location data for DCOs in case of an imminent doping test



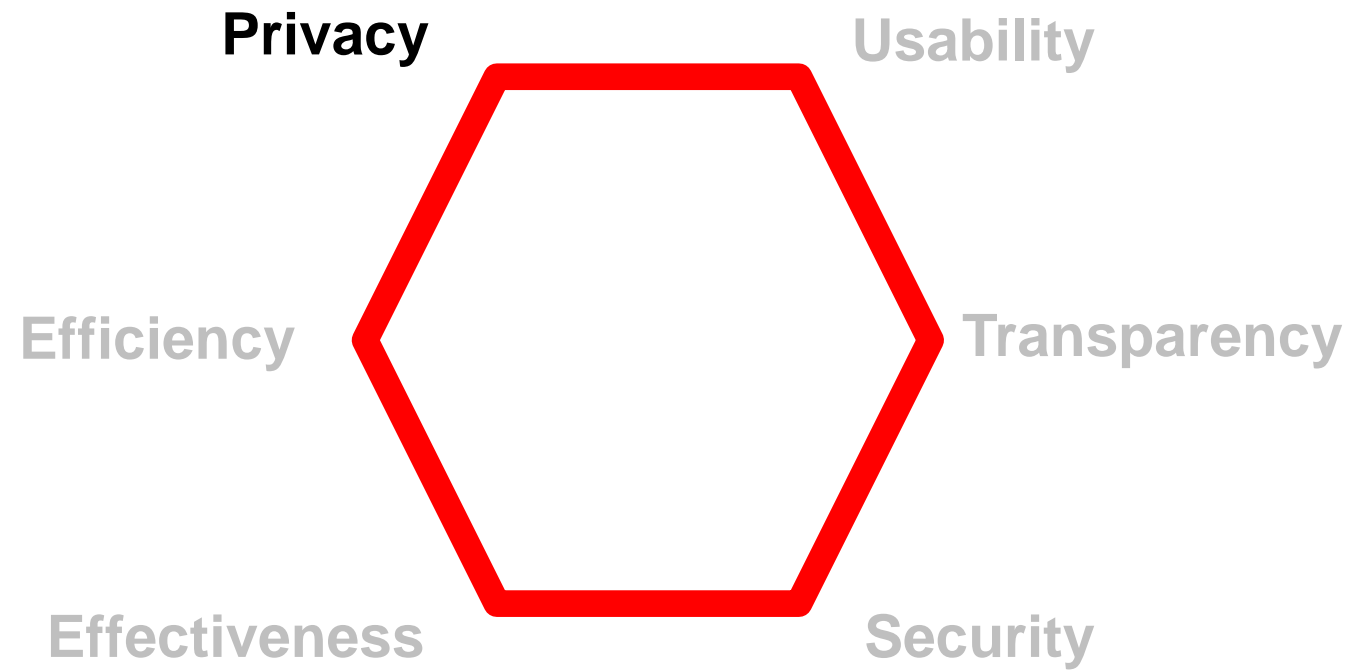




eves - Wearable

- Dedicated Hardware
- SMS-based → useable worldwide
- AES-256 encrypted text messages
- Own software on device
- Hardware from uBlocks and other vendors
- 1st prototype using Cell-ID and GPS positioning
- 2nd prototype is under development, including additional A-GPS, maybe WiFi positioning





Location Information on a Need-to-Know Basis

PARADISE-Demo

Secure https://demo.privacy-paradise.de/dco/orders/CTLI2006

Abmelden

1. Feb 2017 - 18. Feb 2017

CTLI2006

Urin

Weitsprung (IAAF)

Ablehnen x

Felix Glockner

Kontrollzeitraum

Auftragsnummer

+491779987234

Testart(en)

Sportart und Verband

KONTROLLAUFRÄGE 0

HISTORIE

Position Anfragen

Position Senden

Map of Berlin showing the city outline and surrounding areas. The map includes labels for various districts and landmarks, such as Charlottenburg, Moabit, and Prenzlauer Berg. The Spree river is visible flowing through the city. The map is sourced from Leaflet and OpenStreetMap contributors.

Location Information on a Need-to-Know Basis

PARADISE-Demo

Secure <https://demo.privacy-paradise.de/dco/orders/CTLI2006>

Abmelden

1. Feb 2017 - 18. Feb 2017
Kontrollzeitraum

CTLI2006
Auftragsnummer

+491779987234
Urin
Testart(en)

Weitsprung (IAAF)
Sportart und Verband

Ablehnen x

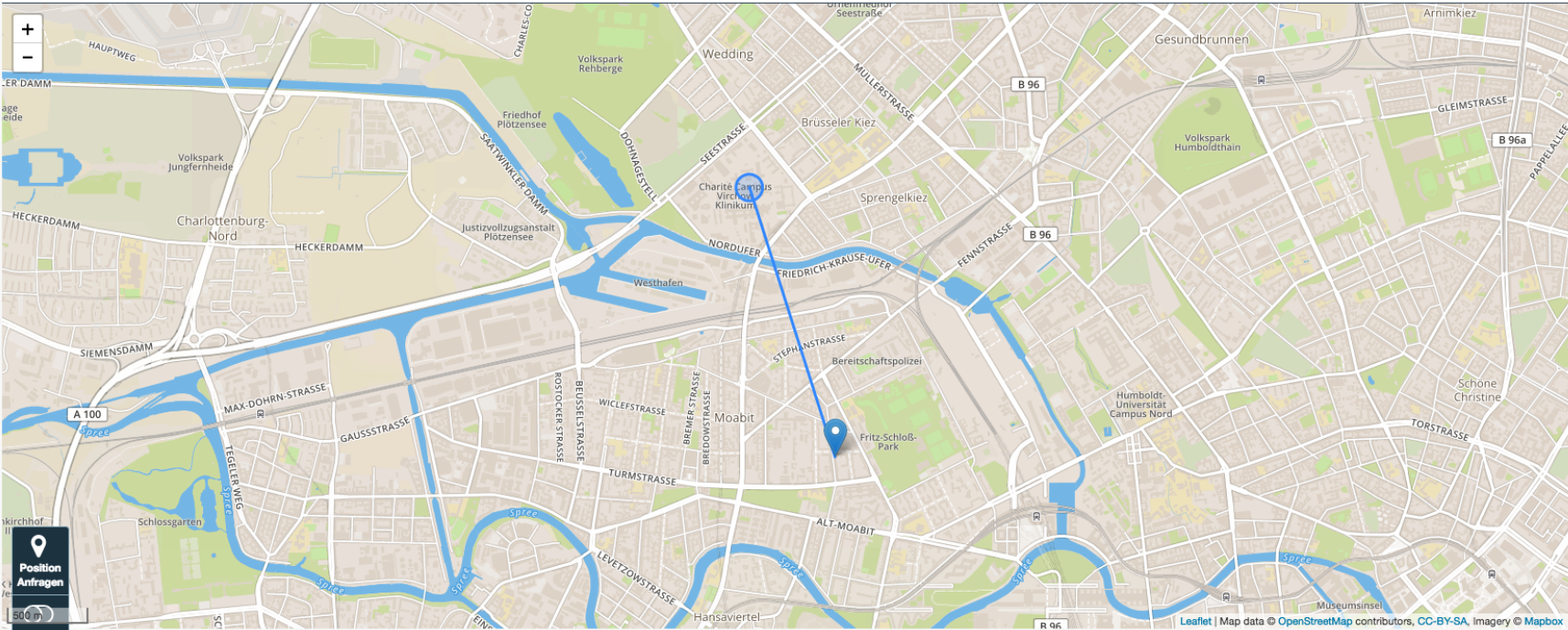
Felix Glockner

KONTROLLAUFRÄGE 0

HISTORIE

Position Anfragen

Position Senden



Leaflet | Map data © OpenStreetMap contributors, CC-BY-SA, Imagery © Mapbox

WhereCamp | PARADISE - Privacy-enhancing Technologies in a Doping Control Use-Case

Location Information on a Need-to-Know Basis

PARADISE-Demo

Secure <https://demo.privacy-paradise.de/dco/orders/CTLI2006>

Abmelden

DCO
Julian Quandt

KONTROLLAUFRÄGE 0

HISTORIE

Felix Glockner

1. Feb 2017 - 18. Feb 2017
Kontrollzeitraum

CTLI2006
Auftragsnummer

+491779987234

Urin
Testart(en)

Weitsprung (IAAF)
Sportart und Verband

Ablehnen x

Athlet
GPS: Lat: 52.542741, Lng: 13.343897, Qualität: 80m, Zeit: Thu Jan 05 2017 16:13:40 GMT+0100 (CET)
GSM: Lat: 52.542741, Lng: 13.343897, Qualität: 500m, Zeit: Thu Jan 05 2017 16:13:45 GMT+0100 (CET)
Batterie: 34
Status: FINISHED

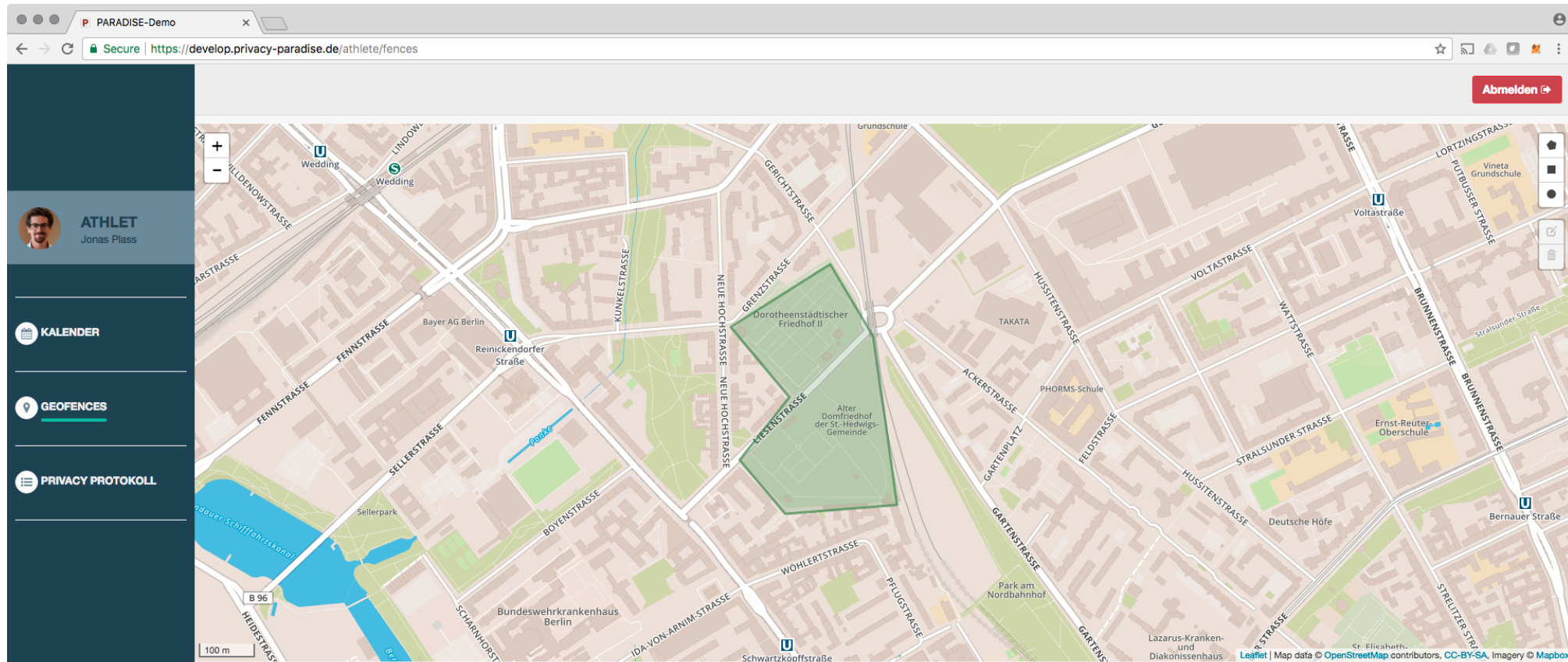
Charité Campus Virchow Klinikum

Position Anfragen

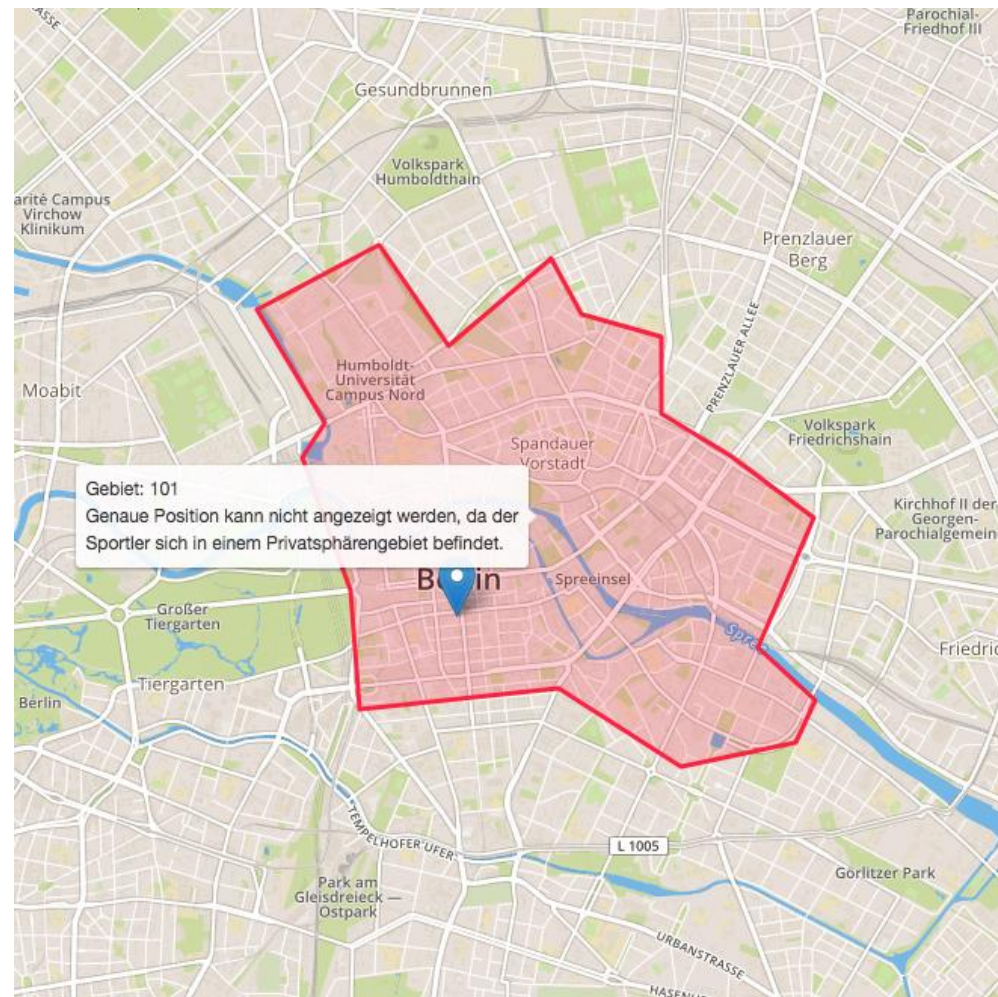
Position Senden

WhereCamp | PARADISE - Privacy-enhancing Technologies in a Doping Control Use-Case

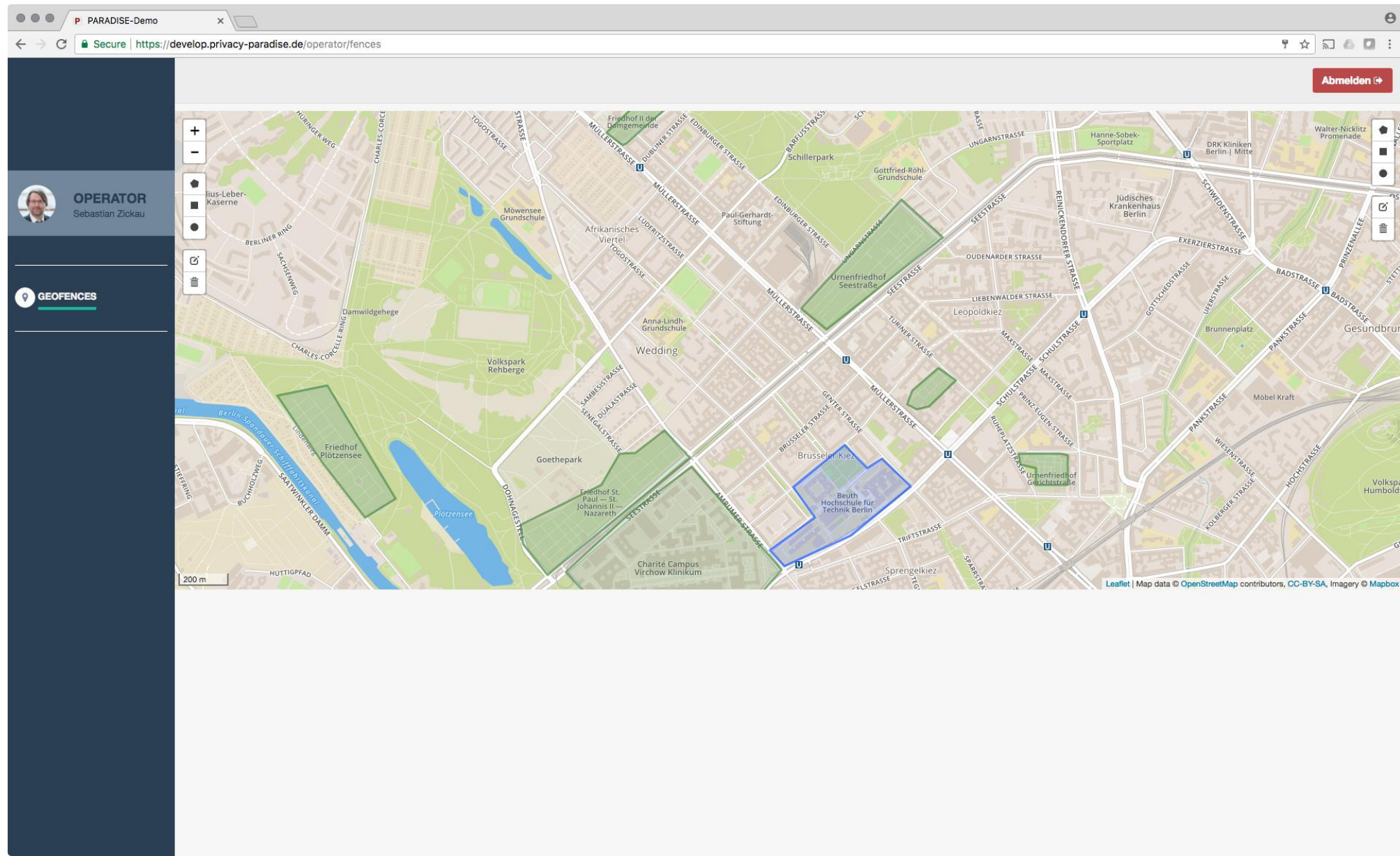
Personal Privacy Areas (self-determination)



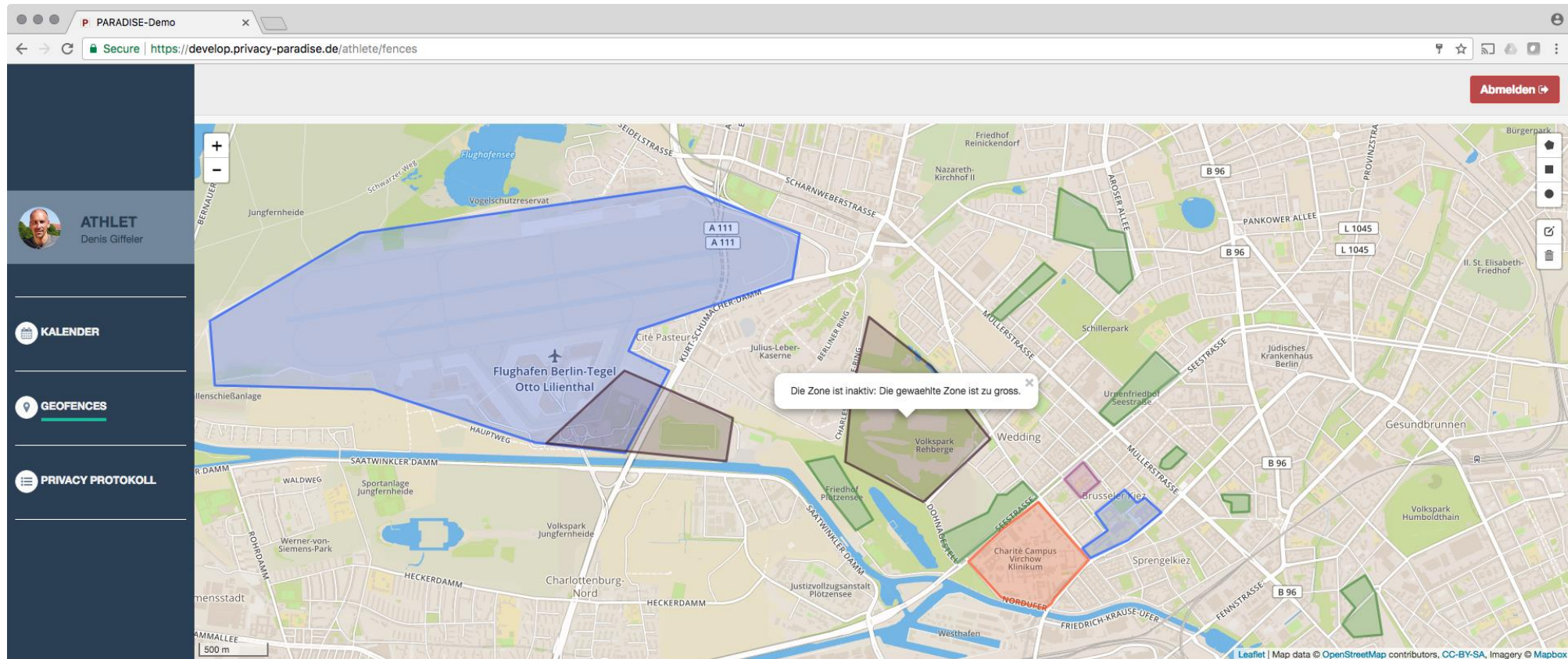
Personal Privcy Areas: Athlete's Definition and DCO's view



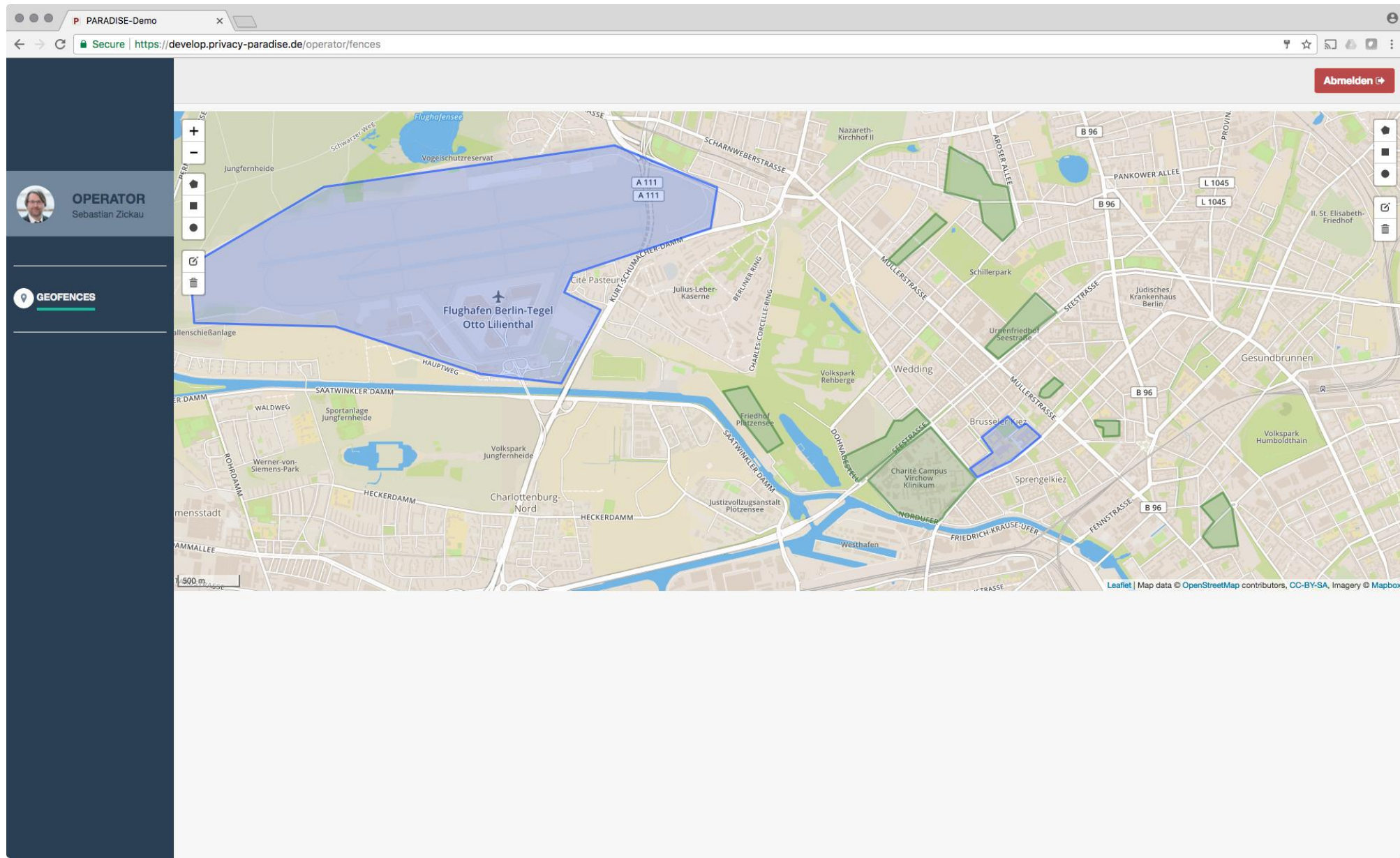
General Privacy Areas Examples

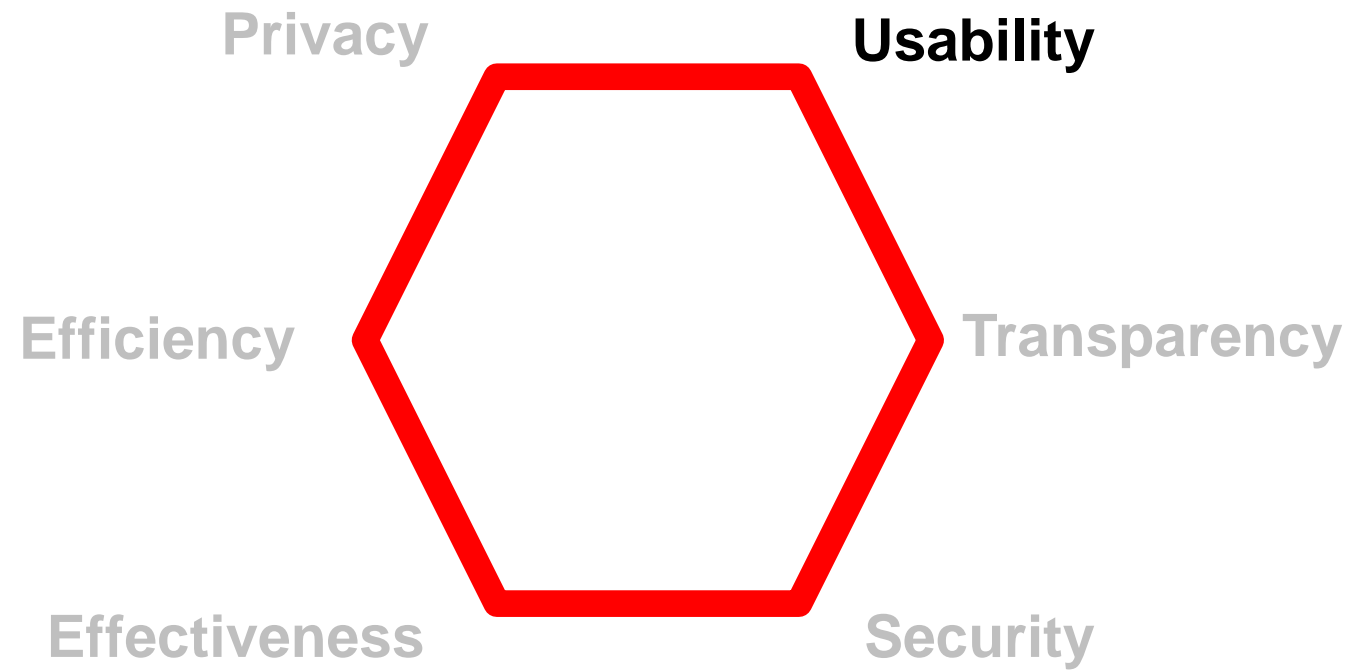


Privacy Areas are limited in Size and Amount



Exclusion Areas





For Athletes

- Fewer data input for athletes
- Data input required less often
- More flexibility for athletes and their daily whereabouts
 - Location changes
- More intuitive interface and interaction

Less Whereabouts Data

PARADISE-Demo

Secure | <https://develop.privacy-paradise.de/athlete/calendar>







Abmelden

ATHLET
Jonas Plass

KALENDER

GEOFENCES

PRIVACY PROTOKOLL

Ort	Von	Bis	Aktion
Hamburg	2017-10-01	2017-10-10	 
Bonn	2017-10-11	2017-10-20	 
Berlin	2017-10-12	2017-10-31	 

- More accurate whereabouts data
- Up-to-date location information
- Could be used together with a car navigation system
 - Including: privacy navigation ideas

For DCO

PARADISE-Demo

Secure | <https://develop.privacy-paradise.de/dco/orders/CTLI5001>

Abmelden

Jonas Plass

27. Okt 2017 - 5. Nov 2017

CTLI5001

Auftragsnummer

+4915153002472

Urin + EPO

Testart(en)

400m (IAAF)

Sportart und Verband

Ablehnen

KONTROLLAUFRÄGE 3

HISTORIE

Athlet

GPS: Lat: 52.542741, Lng: 13.343897, Qualität: 80m, Zeit: Thu Jan 05 2017 16:13:40 GMT+0100 (CET)

GSM: Lat: 52.542741, Lng: 13.343897, Qualität: 500m, Zeit: Thu Jan 05 2017 16:13:45 GMT+0100 (CET)

Batterie: 34

Status: FINISHED

Charité Campus Virchow Klinikum

Position Anfragen

Position Senden







Leaflet | Map data © OpenStreetMap contributors, CC-BY-SA, Imagery © Mapbox

For DCO - Clear Overview

PARADISE-Demo

Secure | <https://develop.privacy-paradise.de/dco/orders>

Abmelden

Name	Kontrollzeitraum	Auftragsnummer	Status
 Jonas Plass	27. Okt 2017 - 5. Nov 2017	CTLI5001	 NEU
 Denis Giffeler	29. Okt 2017 - 5. Nov 2017	CTLI5002	 NEU
 Clemens Putschli	29. Okt 2017 - 5. Nov 2017	CTLI5003	 NEU

DCO
Sebastian Zickau

KONTROLLAUFRÄGE 3

HISTORIE


NADO/DCO Calendar View

PARADISE-Demo x

Secure https://demo.privacy-paradise.de/dco/orders/CTLI2006


Abmelden

←

 **DCO**
Julian Quandt

1. Feb 2017 - 18. Feb 2017
Kontrollzeitraum

CTLI2006
Auftragsnummer

 +491779987234

Urin
Testart(en)

Weitsprung (IAAF)
Sportart und Verband

Ablehnen x

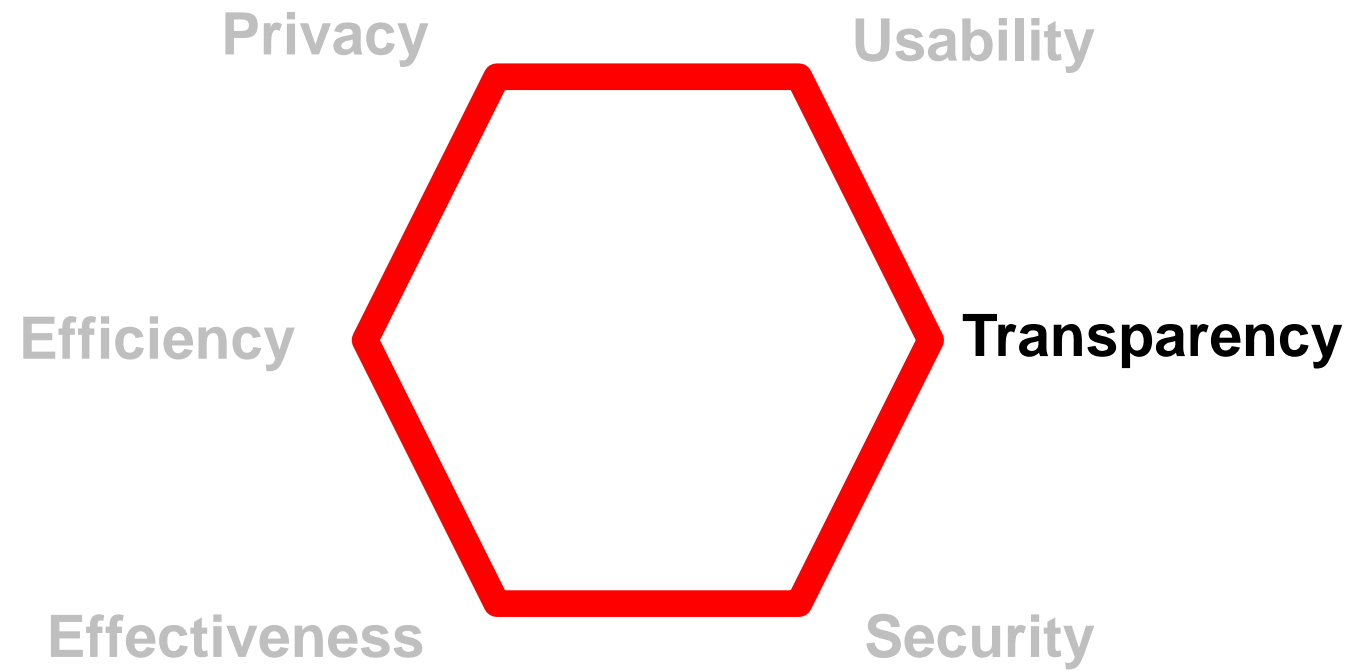
KONTROLLAUFRÄGE 0

HISTORIE

Februar 2017

Montag	Dienstag	Mittwoch	Donnerstag	Freitag	Samstag	Sonntag
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	1	2	3	4	5

● Berlin



Transparency

PARADISE-Demo

Secure | <https://develop.privacy-paradise.de/athlete/log>

Abmelden

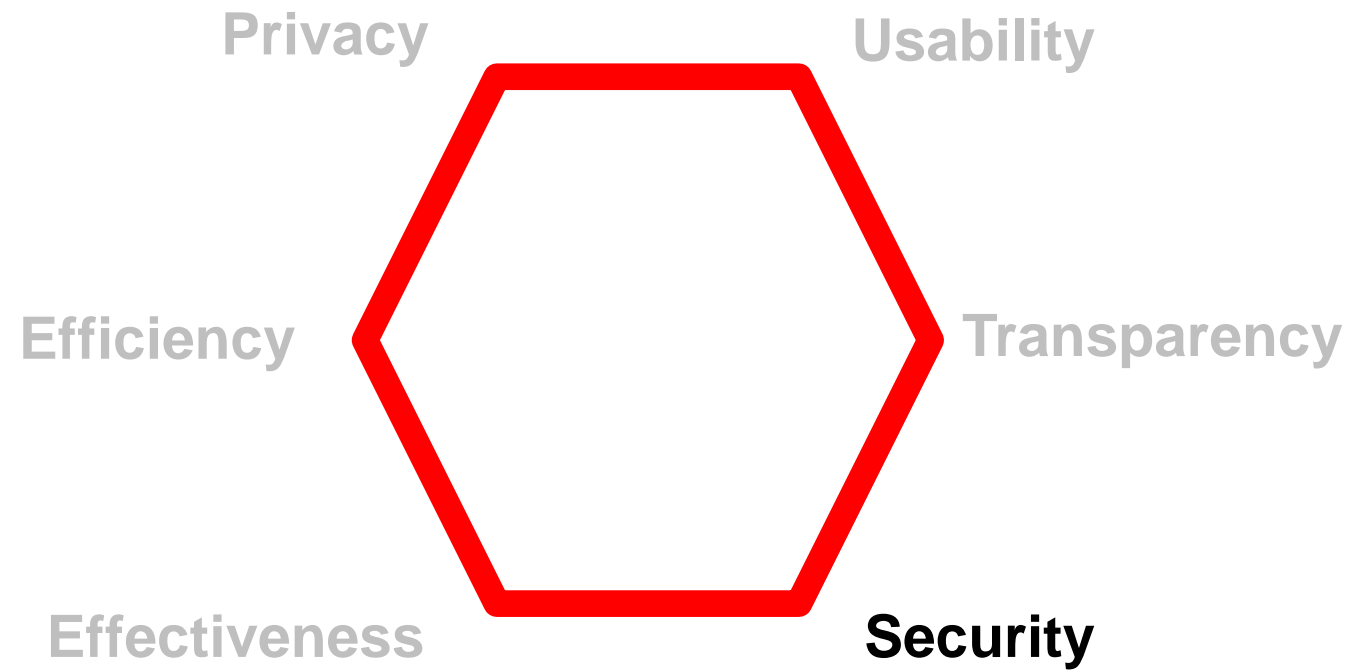
ATHLET
Jonas Plass

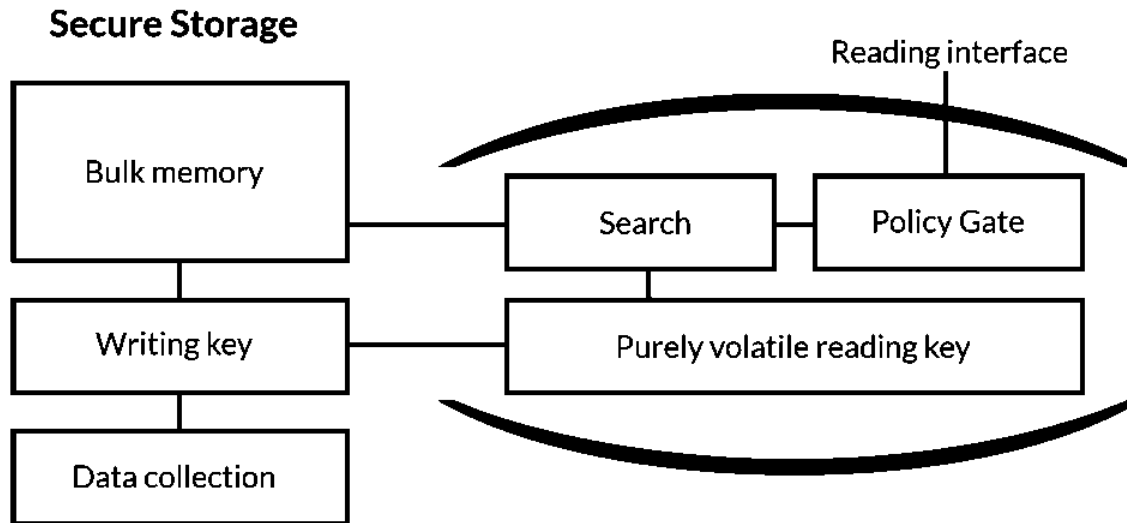
KALENDER

GEOFENCES

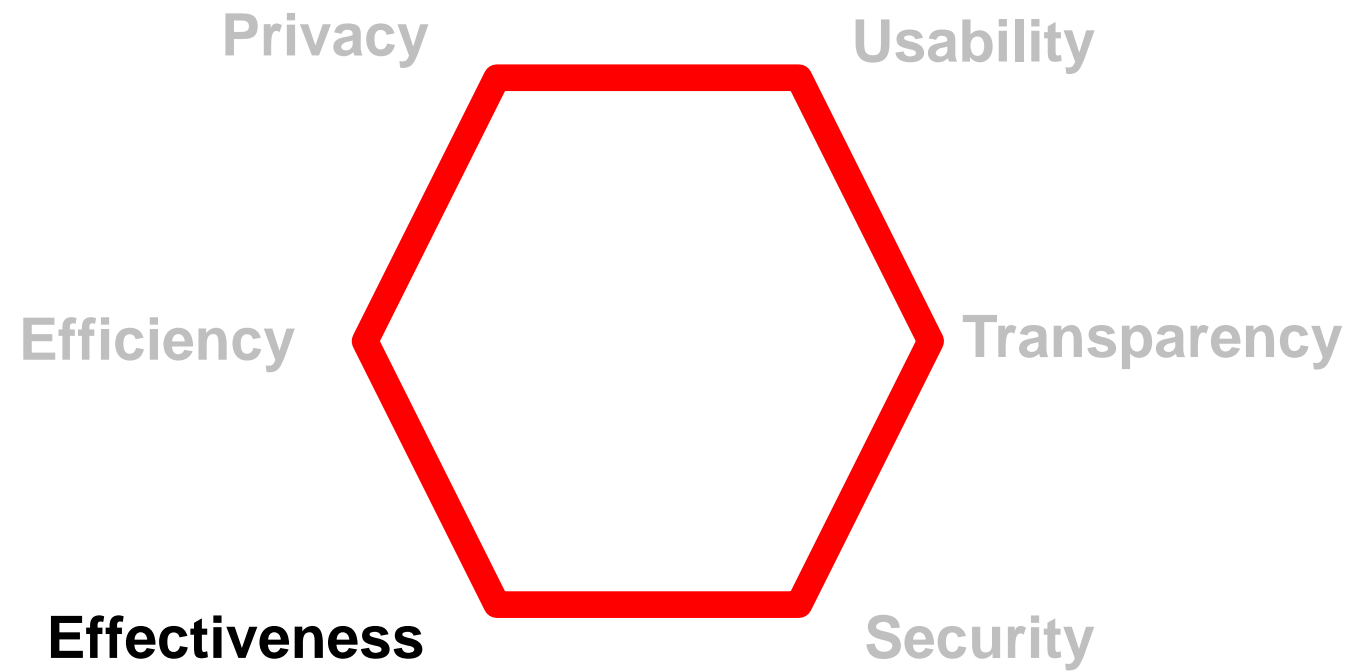
PRIVACY PROTOKOLL

KONTROLL-ID	AKTION	ZEITPUNKT
CTLI1000	POSITION	26. Januar 2017 0:00
CTLI1000	POSITION	25. Februar 2017 13:21
CTLI1000	POSITION	27. Februar 2017 22:09
CTLI1000	POSITION	27. Februar 2017 22:17
CTLI1000	POSITION	28. Februar 2017 9:11



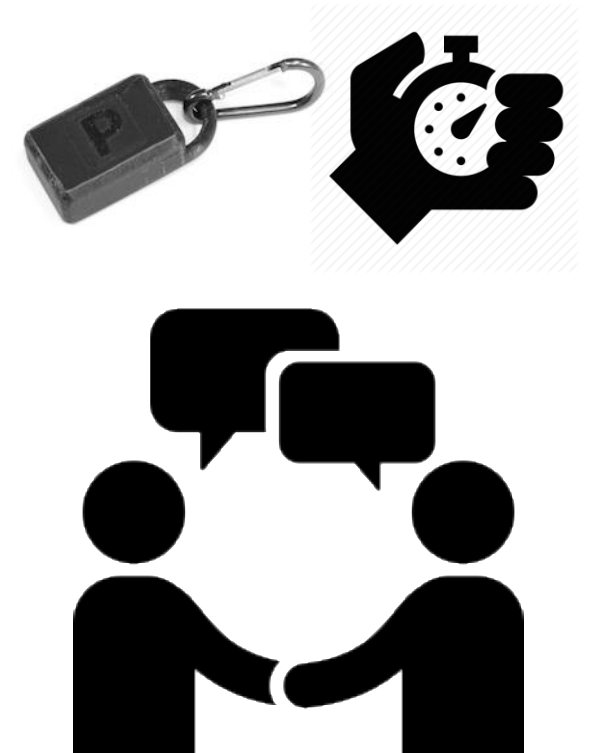


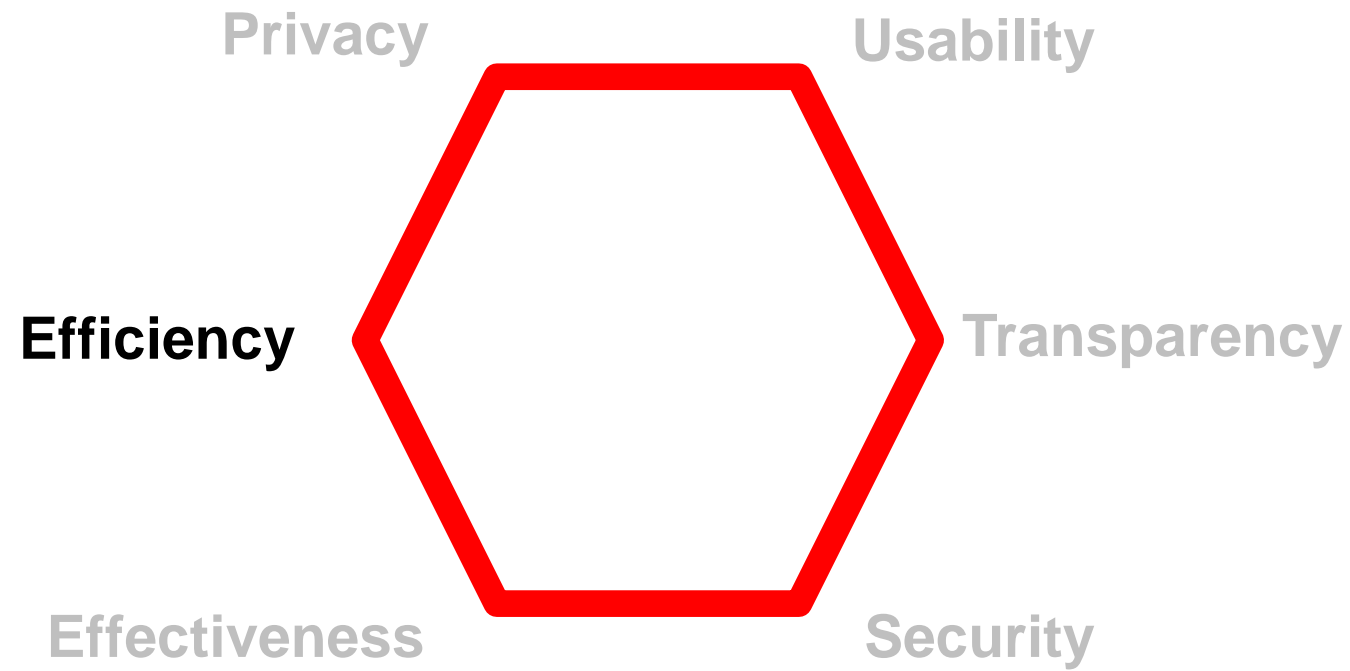
- Attribute-based Access Control
- Attribute-based Delegation
- Privacy-preserving Location-based Access Control using geofences
- Encrypted text messages
- No 3rd-party services necessary
- Sealed-Cloud technologies
 - Data Cleanup Areas
 - No administrator access



EFFECTIVENESS

- Controls become potentially possible all day long
- Probability of doping control is equally distributed throughout the day
- From an athletes perspective:
 - Fairness: Every athlete should be treated equally
- Usable worldwide
- Time can be reduced between phone call and meet-up





Mobile Application Shortcomings

- Android prototype was developed
- Not in control of the hardware
- Reactive approach difficult
- Dependent on iOS and Android APIs and operating systems
- Easier to manipulate (e. g., spoofing locations and detecting requests)

- Those derogations should **in particular apply to data transfers required and necessary for important reasons of public interest**, for example in cases of international data exchange between competition authorities, tax or customs administrations, between financial supervisory authorities, between services competent for social security matters, or for public health, for example in the case of contact tracing for contagious diseases or **in order to reduce and/or eliminate doping in sport.**

PARADISE Summary

- Privacy-driven from an athlete's perspective
- Dedicated eves-Device
- Spontaneous whereabouts changes
- Reduces data being collected and used
- Uses new ideas, such as:
 - Privacy areas (self-determination)
 - Provides information on a need-to-know basis
- Adds additional security features
- Point in time for testing and location data quality is equally distributed
- Reduces time between phone-call and meet-up

THANK YOU – ANY QUESTIONS, PLEASE

Contact

Dr. Denis Giffeler

dg@gekko.de

gekko mbH

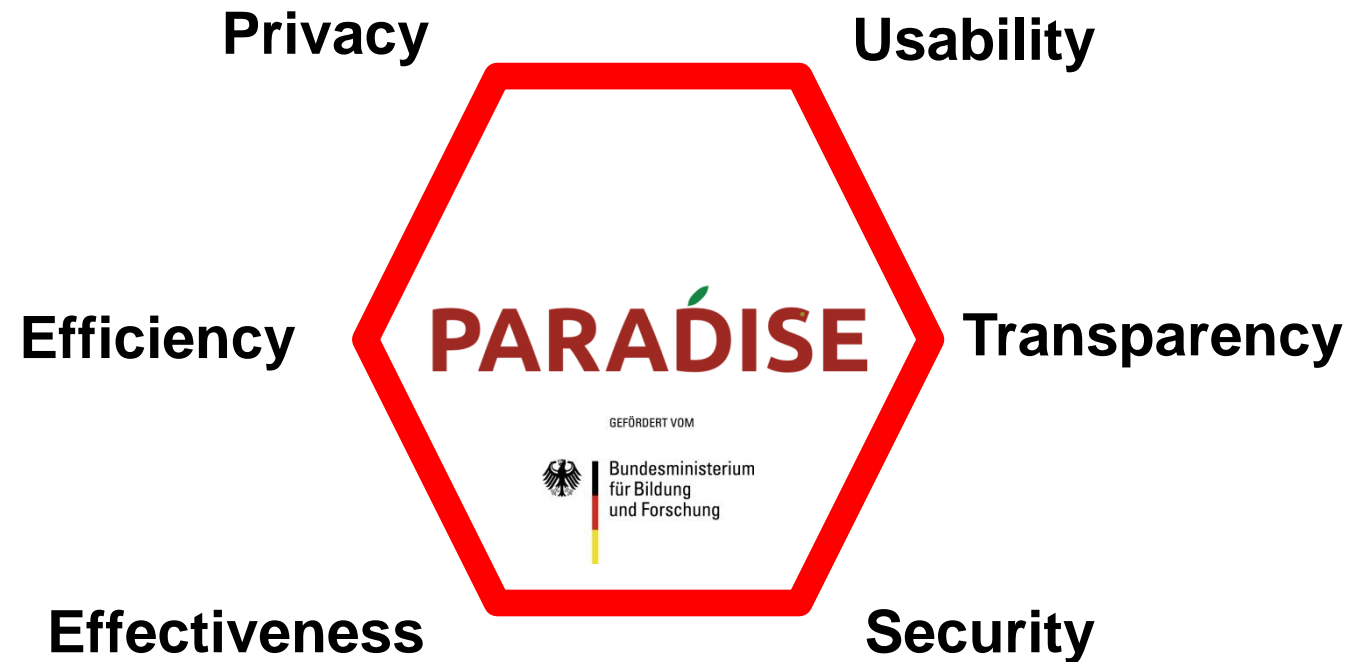
Dipl.-Inform. Sebastian Zickau

sebastian.zickau@tu-berlin.de

TU Berlin | T-Labs

Service-centric Networking

www.snet.tu-berlin.de



PARADISE Projekt: www.privacy-paradise.de

