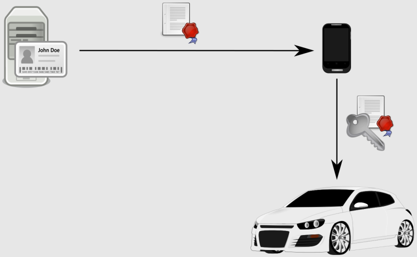
Technische Universität Braunschweig

Institute of Operating Systems and Computer Networks

V-CHARGE



Secure Smartphone-based Registration and Key Deployment for Vehicle-to-Cloud Communications

Workshop on Security, Privacy and Dependability for Cyber Vehicles (CyCAR)

Julian Timpner, Dominik Schürmann, Lars Wolf, 4. November 2013

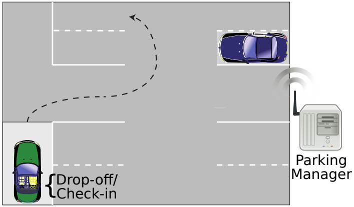
Motivation

V-Charge

- Autonomous valet parking with e-mobility
- Electric vehicles, equipped with affordable sensor systems
- No Internet access on vehicles (parking garage)

Challenges

- Minimum of infrastructure (DTN)
- Efficiently using charging resources
- Multiple communication channels (V2C, Web, mobile)



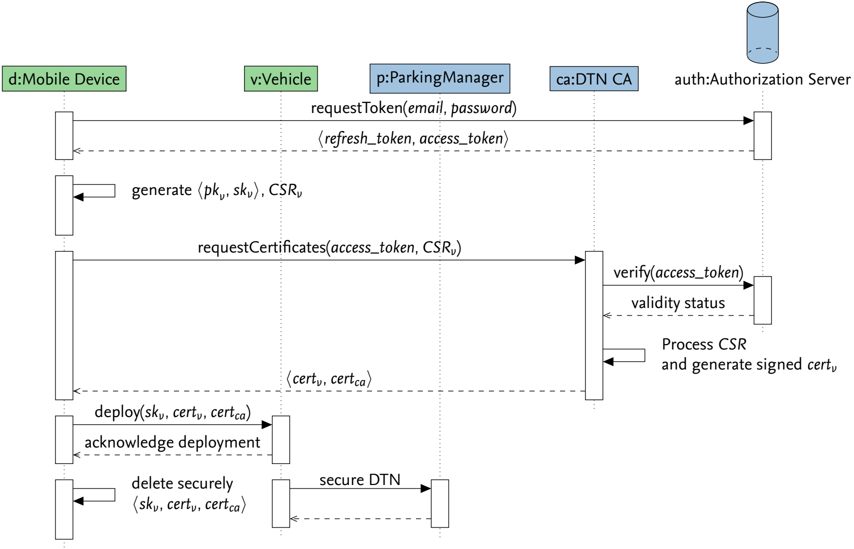
This Talk

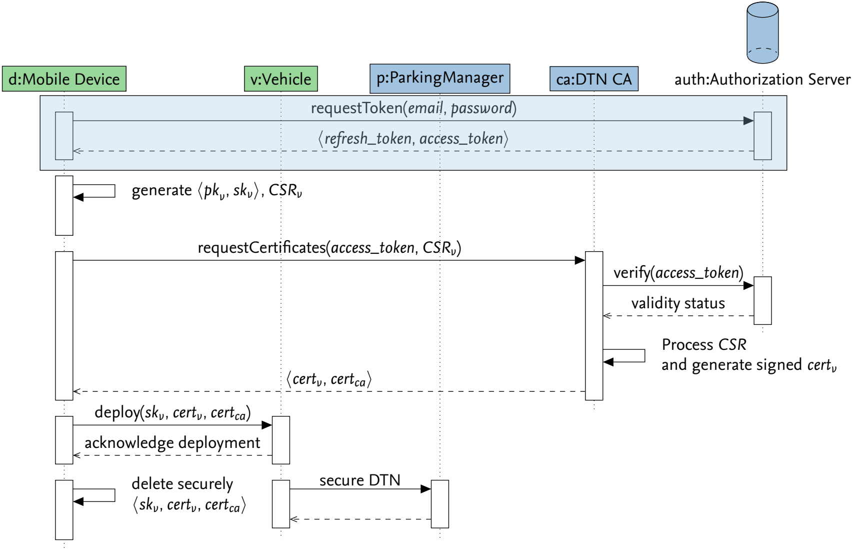
Security Challenges

- Vehicle registration process independently of OEMs
- Key generation and deployment, while minimizing trust in central authorities

Secure smartphone-based registration and key deployment

- Framework can be used by vehicle owners at any time
- Key generation solely done by vehicle owner on a mobile device
- Vehicle registration on mobile device based on well-researched PKI
- No proprietary protocols involved


d:Mobile Device
v:Vehicle
p:ParkingManager
ca:DTN CA
auth:Authorization Server
requestToken(*email*, *password*)
⟨*refresh_token*, *access_token*⟩
generate ⟨pk_v, sk_v⟩, CSR_v
requestCertificates(*access_token*, CSR_v)
verify(*access_token*)
validity status
Process *CSR*
and generate signed $cert_v$
⟨$cert_v$, $cert_{ca}$⟩
deploy(sk_v, $cert_v$, $cert_{ca}$)
acknowledge deployment
delete securely
⟨sk_v, $cert_v$, $cert_{ca}$⟩
secure DTN


d:Mobile Device
v:Vehicle
p:ParkingManager
ca:DTN CA
auth:Authorization Server
requestToken(*email*, *password*)
$\langle$*refresh_token*, *access_token*$\rangle$
generate $\langle pk_v, sk_v \rangle$, CSR_v
requestCertificates(*access_token*, CSR_v)
verify(*access_token*)
validity status
Process *CSR*
and generate signed $cert_v$
$\langle cert_v, cert_{ca} \rangle$
deploy(sk_v, $cert_v$, $cert_{ca}$)
acknowledge deployment
delete securely
$\langle sk_v, cert_v, cert_{ca} \rangle$
secure DTN

Smartphone-to-Cloud: Authentication/Authorization

Requirements

- Don’t store account passwords on device (protection against theft)
- Easy revocation of devices (recovery after theft)
- Don’t force users to repeatedly login before usage (usability)
- Based on open standards

Smartphone-to-Cloud: Authentication/Authorization

Requirements

- Don’t store account passwords on device (protection against theft)
- Easy revocation of devices (recovery after theft)
- Don’t force users to repeatedly login before usage (usability)
- Based on open standards

OAuth 2.0

- Provides authorization for Web services and mobile devices
- RFC 6749, 6750, 6819
- Heavy standard, some say “over-engineered”

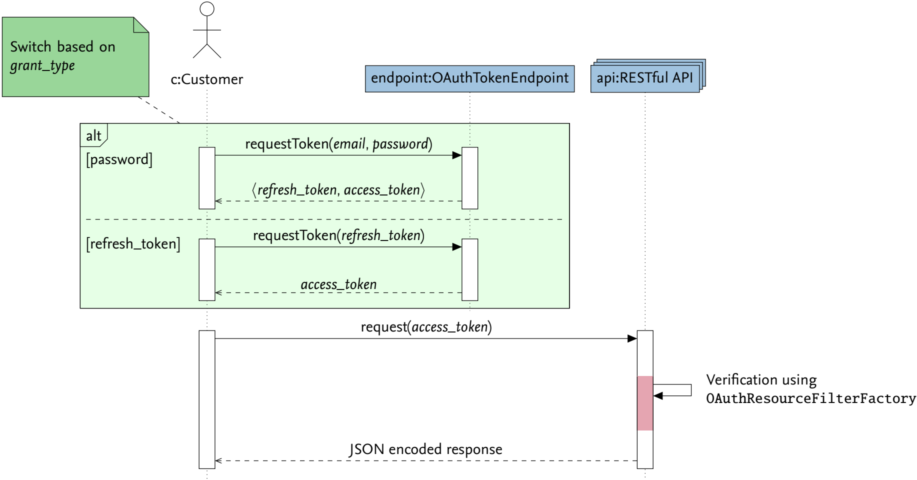
OAuth 2.0 Subset

Authentication/Authorization

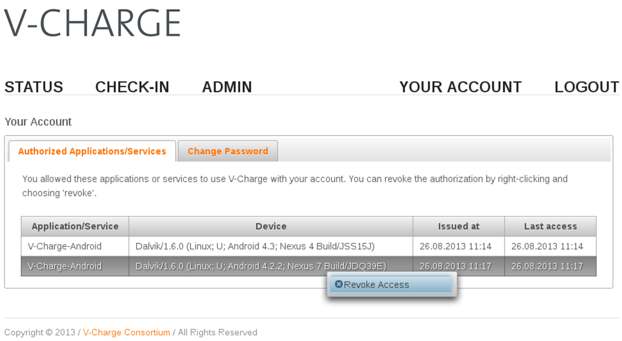
- No third-party applications planned for V-Charge
- No redirection flow based on *grant_type* “authorization_code”
- Reducing protocol complexity
- RESTful JSON interface, OAuth based on Apache Oltu

Concept	**Description**
Token Endpoint	HTTP service to request tokens
grant_type	our subset implements “password” and “refresh_token”
refresh_token	long living authorization token
access_token	limited access token

OAuth 2.0 Subset


Switch based on *grant_type*
c:Customer
endpoint:OAuthTokenEndpoint
api:RESTful API
alt
[password]
requestToken(*email*, *password*)
⟨*refresh_token*, *access_token*⟩
[refresh_token]
requestToken(*refresh_token*)
access_token
request(*access_token*)
Verification using
OAuthResourceFilterFactory
JSON encoded response

Device Revocation



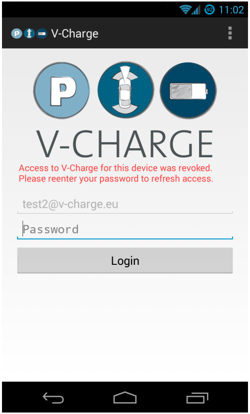
V-CHARGE

Your Account

You allowed these applications or services to use V-Charge with your account. You can revoke the authorization by right-clicking and choosing 'revoke'.

Application/Service	Device	Issued at	Last access
V-Charge-Android	Dalvik/1.6.0 (Linux; U; Android 4.3; Nexus 4 Build/JSS15J)	26.08.2013 11:14	26.08.2013 11:14
V-Charge-Android	Dalvik/1.6.0 (Linux; U; Android 4.2.2; Nexus 7 Build/JDQ39E)	26.08.2013 11:17	26.08.2013 11:17

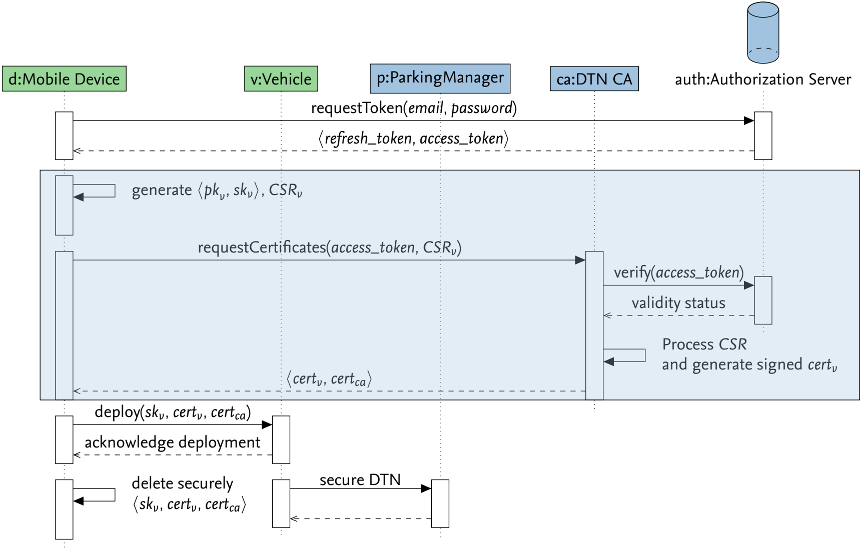
Copyright © 2013 / V-Charge Consortium / All Rights Reserved



Access to V-Charge for this device was revoked. Please reenter your password to refresh access.

test2@v-charge.eu

Password


d:Mobile Device
v:Vehicle
p:ParkingManager
ca:DTN CA
auth:Authorization Server
requestToken($email$, $password$)
$\langle refresh\_token, access\_token \rangle$
generate $\langle pk_v, sk_v \rangle$, CSR_v
requestCertificates($access\_token$, CSR_v)
verify($access\_token$)
validity status
Process CSR
and generate signed $cert_v$
$\langle cert_v, cert_{ca} \rangle$
deploy(sk_v, $cert_v$, $cert_{ca}$)
acknowledge deployment
delete securely
$\langle sk_v, cert_v, cert_{ca} \rangle$
secure DTN

Vehicle Registration

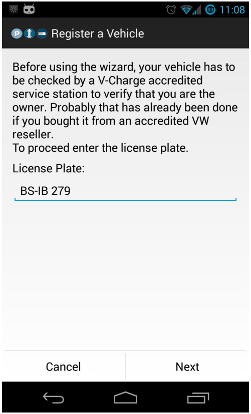
Registration

- Easy registration process executable by customers
- Vehicle Identification Number (VIN)
- Registration of vehicles without the need of in-vehicle display and in-vehicle Internet connection

Key generation

- Nobody but the owner possesses the private key
- Generation on mobile device, protected by OS security
- Enough entropy compared to embedded hardware

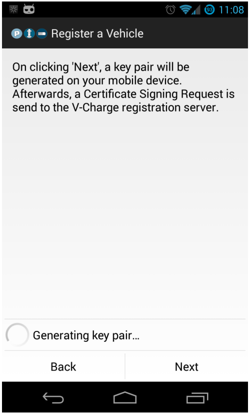
Vehicle Registration



Before using the wizard, your vehicle has to be checked by a V-Charge accredited service station to verify that you are the owner. Probably that has already been done if you bought it from an accredited VW reseller.
To proceed enter the license plate.

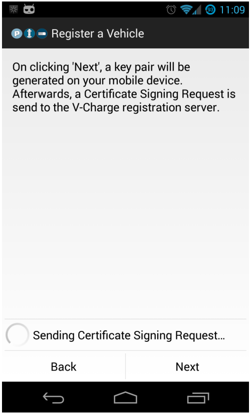
License Plate:

BS-IB 279



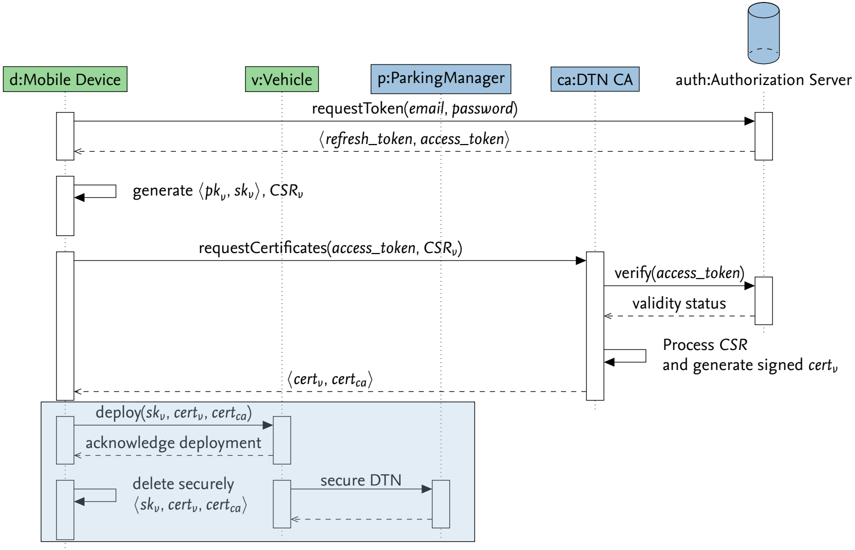
On clicking 'Next', a key pair will be generated on your mobile device. Afterwards, a Certificate Signing Request is send to the V-Charge registration server.

Generating key pair...



On clicking 'Next', a key pair will be generated on your mobile device. Afterwards, a Certificate Signing Request is send to the V-Charge registration server.

Sending Certificate Signing Request...


d:Mobile Device
v:Vehicle
p:ParkingManager
ca:DTN CA
auth:Authorization Server
requestToken(*email*, *password*)
⟨*refresh_token*, *access_token*⟩
generate ⟨pk_v, sk_v⟩, CSR_v
requestCertificates(*access_token*, CSR_v)
verify(*access_token*)
validity status
Process *CSR*
and generate signed $cert_v$
⟨$cert_v$, $cert_{ca}$⟩
deploy(sk_v, $cert_v$, $cert_{ca}$)
acknowledge deployment
delete securely
⟨sk_v, $cert_v$, $cert_{ca}$⟩
secure DTN

Key Deployment

Requirements

- In-vehicle Hardware Security Module (HSM)
- NFC-enabled mobile device

Deployment process (only conceptual)

- Transmission of $\langle sk_v, cert_v, cert_{ca} \rangle$ over NFC-SEC to HSM
- Delete $\langle sk_v, cert_v, cert_{ca} \rangle$ from device

Hardware Security Modules

- Hardware implementation details are beyond the scope of our paper
- API: Mode to reset its memory and a deployment mode to store new $\langle sk_v, cert_v \rangle$-pairs
- Vehicles are equipped with HSM by service stations or car manufacturers
- Require PIN to access the API
- NFC with security layer or NFC-SEC

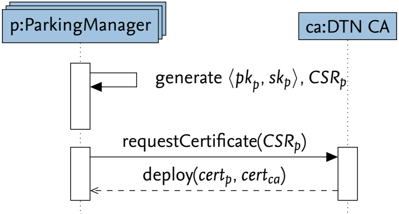
DTN Security

Implementation

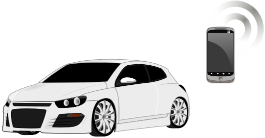
- IBR-DTN daemon
- Cloud-to-Vehicle security based on RFC 6257
- TLS on TCP convergence layer

V-Charge key management design

- PKI with certificates
- Revocation by “floating” CRLs


p:ParkingManager
ca:DTN CA
generate $\langle pk_p, sk_p \rangle$, CSR_p
requestCertificate(CSR_p)
deploy($cert_p$, $cert_{ca}$)

Remote Attacks



Intercept *access_token*

- Attack on TLS with pinned certificate

Eavesdropping/replay attacks on NFC

- NFC-SEC standard
- Transmission only happens once, as opposed to vehicular access control systems

Attacking the Application

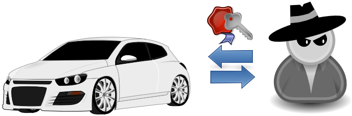
Extract *refresh_token*

- Malicious application attacking Android's *AccountManager* (root exploit needed)
- Revocation on device theft

Steal sk_v before deployment

- Privilege escalation to gain access to Unix user of V-Charge app
- sk_v is stored only for a short duration on smartphone

Attacks Involving the Vehicle



Deploy attacker's $\langle sk_t, cert_t \rangle$ to a victim's vehicle

- HSM should only accept $cert_t$ if it is issued for the corresponding VIN_v of the vehicle

Extract $\langle sk_v, cert_v \rangle$ from a victim's vehicle

- Requires hacking the HSM
- Revocation of $cert_v$, re-generate sk_v, request a new $cert_v$

Conclusion

- Novel approach for securely deploying cryptographic keys to vehicles
- Supporting multiple services without trusting central authorities
- Private key never leaves vehicle owner
- Authentication/Authorization based on standards
- Overcoming OAuth design problems: keeping it simple
- Usable security
- No vehicular Internet access required

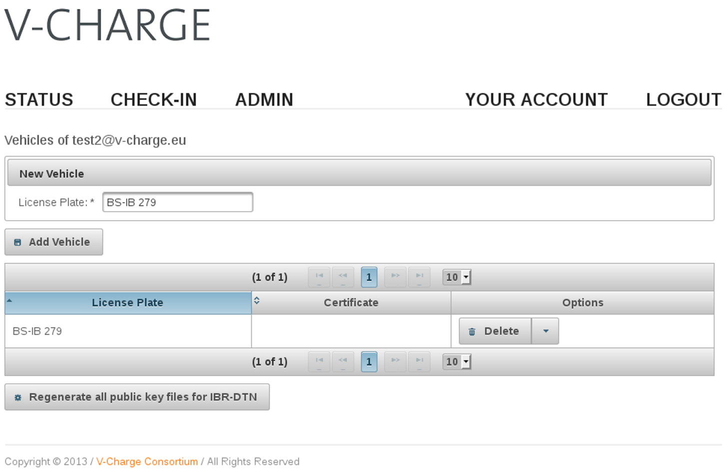
Conclusion

- Novel approach for securely deploying cryptographic keys to vehicles
- Supporting multiple services without trusting central authorities
- Private key never leaves vehicle owner
- Authentication/Authorization based on standards
- Overcoming OAuth design problems: keeping it simple
- Usable security
- No vehicular Internet access required

Questions?

email: `schuermann@ibr.cs.tu-bs.de`

Vehicle Pre-Registration



Vehicles of test2@v-charge.eu

License Plate: * BS-IB 279

License Plate	Certificate	Options
BS-IB 279		Delete

Copyright © 2013 / V-Charge Consortium / All Rights Reserved

Public Key Pinning

- Introducing certificate/public key pinning
- Include V-Charge's SSL CA certificate in-app
- Trust by application updates
- No reliance on CAs

V-Charge Project

Goals

- A system combining autonomous valet parking with e-mobility
- Increasing customer acceptance of electric vehicles
- By compensating for longer charging cycles

Challenges

- Efficiently using scarce charging resources
- Multiple communication channels (V2I, Web, mobile)
- Autonomous driving and parking (not in this talk)

V-CHARGE

V-Charge Partners

CAROLO-WILHELMINA BRAUNSCHWEIG
Technische
Universität
Braunschweig

UNIVERSITY · OF · OXFORD
DOMI NVS ILLV
MINA TIO MEA

SIGILLVM · ALMAE · VNIVERSITATIS · STVDII · PARMENSIS
AVREA PARMA

Motivation

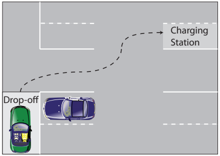
Scenario: EV driver at airport

- Roam for a free spot
- Use shuttle services
- Transport luggage
- What about charging?

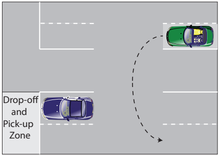
Disadvantages

- Cumbersome
- Only few charging stations
- Makes it even harder to find parking

V-Charge: Autonomous Parking and Charging

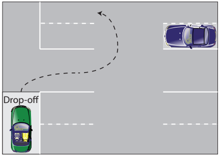


Drop-off

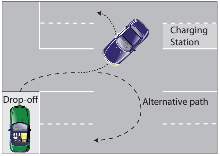


Reparking

V-Charge: Advanced Scenarios



No CS available



Blocked path

TU Contributions

- V2X communications
- Server infrastructure
- Customer interaction
- System security
- Parking resource management