EVS 27 Barcelona, 20.11.2013

Bundesverband Solare Mobilität e.V., as a member of AVERE and AVERE as a member of WEVA, has tabled for discussion and motion:

A proposal of a WorldMobilityCard+Identity (WMC+)

How to use world wide (e-) mobility infrastructures without losing privacy!

Issue 0.1-Draft

Authors:

Andreas Michael Reinhardt, BSM e.V.
Håkan Källberg, Chargepartner GmbH
Frank Thurecht, Chargepartner GmbH
Markus Spiekermann, Moveabout GmbH
Willi Gramberg, OpenLimit SignCubes GmbH
Steffen Sklebitz, OpenLimit SignCubes GmbH

Contact:
http://www.bsm-ev.de/wwmmc-id
wwmmc-id@bsm-ev.de

Date:
November 2013

A proposal of a WorldMobilityCard+Identity (WMC+)

How to use world wide (e-) mobility infrastructures without losing privacy?

Abstract (Andreas-Michael Reinhardt)

The 35th International Conference of Data Protection and Privacy Commissioners held in Warsaw from 23rd to 26th September 2013 urged governments and Internet companies to take effective measures against the ever more comprehensive registration and surveillance. Therefore, Warsaw Conference has adopted several resolutions, among others, on the necessity of an international agreement on data protection, on technical measures against the tracking of the individual use of the Internet ("Do-Not-Track") Barcelona 'EVS27' World Congress 17th - 20th Nov. 2013 is the podium to raise an important question and to invite for worldwide debate during next 24 months in academia, politics and societies: How to travel and to use world wide upcoming Electric Mobility Infrastructures and their Benefits without losing Privacy and Dignity?

The Authors of this White Paper are supporting the Warsaw accord.

In our opinion, EVS27 Congress should adopt a resolution which endorses on the one side the Warsaw resolutions and on the other side should head for an international understanding about a new 'Personal Identity Concept and Manifestation' and its whereabouts, whether Token, Card, Smart device or "software only" driven, which gives advantage to international standardized Multi Mobility Services striving for less private information dispatched to Front- and Backend IT Systems.

How to design by purpose new and lesser Private Data using Interfaces for Electric Vehicle (EV) Charging Stations or Electric Vehicle Supply Equipment (EVSE*) and back-end systems and interfaces (EVSE Operator or Charge Management System.)? This and other questions should be discussed and worldwide agreed following the rule, to avoid by purpose collection of private data when shaping transaction based services and if need for collection to rather anonymize data and pseudonymise when using private data can not be avoided for example driver license checking when hiring a vehicle.

The German Federal Association of Solar Mobility (BSM - Bundesverband Solare Mobilität) - Member of AVERE for Germany - has initiated an Initiative, supported by its members, which heads for international debate and global agreement on private data procession when people are worldwide mobile, for example with electric driven vehicles and using means of transportation from train, tram to bus to car sharing.

*) tc69 international standardization commitee in charge for EV infrastructure has deleted the idiom EVSE in his Barcelona Session for Nov 18 th of 2013

Introduction

Electric Mobility - Paradigm Shift (Markus Spiekermann)

Electric Mobility is a megatrend, emerged within the last years all over the world, as electric mobility provides solutions for the most daring problems in the developed countries and the emerging nations. It has ethical, technical, political and last but not least environmental advantages compared to mobility based on fossil fuel. However, it is more than just exchanging the internal combustion engine (ICE) of a car by an electric engine and a battery. It is a change in mindset - a paradigm shift in mobility is on the horizon as electric mobility is a system approach.

> *Thesis: Electric Mobility as a product is not bound to a certain natural resource, as electricity can be made from several sources. This makes it sustainable and the source exchangeable. The need for Interoperability between the providers of the energy source is obvious*

Most people have an intrinsic wish for mobility, which leads to a huge demand for cars, natural resources and energy in the emerging markets. There have been several approaches to introduce electric mobility in history, but they never succeeded, as the ease of use, the range and the convenience in owning an own ICE based car have been too big disadvantages in the past.

Today, the chances for the success of the electricity based mobility are better than ever. This is due to some trends:

- The environmental concerns and the related lifestyle of green living and sustainability have become mainstream.
- Renewable, but volatile energy is widely accepted and fostered by politics
- The advantages of owning a car in an urban setting are more and more outweighed by practical and financial burdens of taking care for this car.
- Digital natives are familiar with a “network thinking” and sharing of resources (eg. server clouds) and service offerings (Software as a Service, eg. Music streaming)

“Shareconomy” is a new buzzword, that describes these trends in one term.

There are still some obstacles to overcome, if electric mobility shall be a valid alternative to fossil based mobility. Technically, an EV has a limited range and a longer process of regaining this range. The energy density of electric storage devices (batteries) is lower than that of chemical storages (petrol, diesel, gas). Therefore less energy can be stored in a given volume (tank vs. battery). The charging of an EV battery takes longer than to refill

the gas tank of the car, especially in respect to the range that can be added in a given time.

> *Thesis: An electric car needs to be recharged more often than an ICE car. Therefore the network of recharging points needs to be more dense.*

The production volume of electric cars is still low, compared to the volume of cars with ICE. Therefore the car producers offer electric cars at relatively higher prices. The financial institutions, eg. leasing banks, are not familiar with residual values of EVs. Caused by this, the leasing and financing costs of EVs are high. Most of the cars owned by users owned in metropolitan areas, are utilized only one hour per day.

> *Thesis: The utilization of the cars should be improved to share and optimize the costs and risks of the pioneer users.*

These trends can be used to solve the above stated points, eg. by sharing infrastructure. It is a task for the economic system and not for a single person or company to build up the necessary infrastructure. But if several suppliers compete and work together on the market for mobility and the related energy supply, standards need to be imposed to allow for interoperability.
New Mobility offerings for the user come along in several possible dimensions and breeds.
If these scenarios shall come true, the characteristics of the stakeholders in the related processes need to be identified.

To simplify these processes for the end user so that he will be able to use only one Device (smartphone or RFID card) to use all characteristics of eMobility and make them secure from the sight of data protection a secure personal identification technique should be used. To be sure that no individual (business) interests bursts this data protection an independent registrar in form of a foundation should be founded as root ancestor to create the IDs.

The following figure shows the relations of card/smartphone identifiers in the WorldMobility-Network

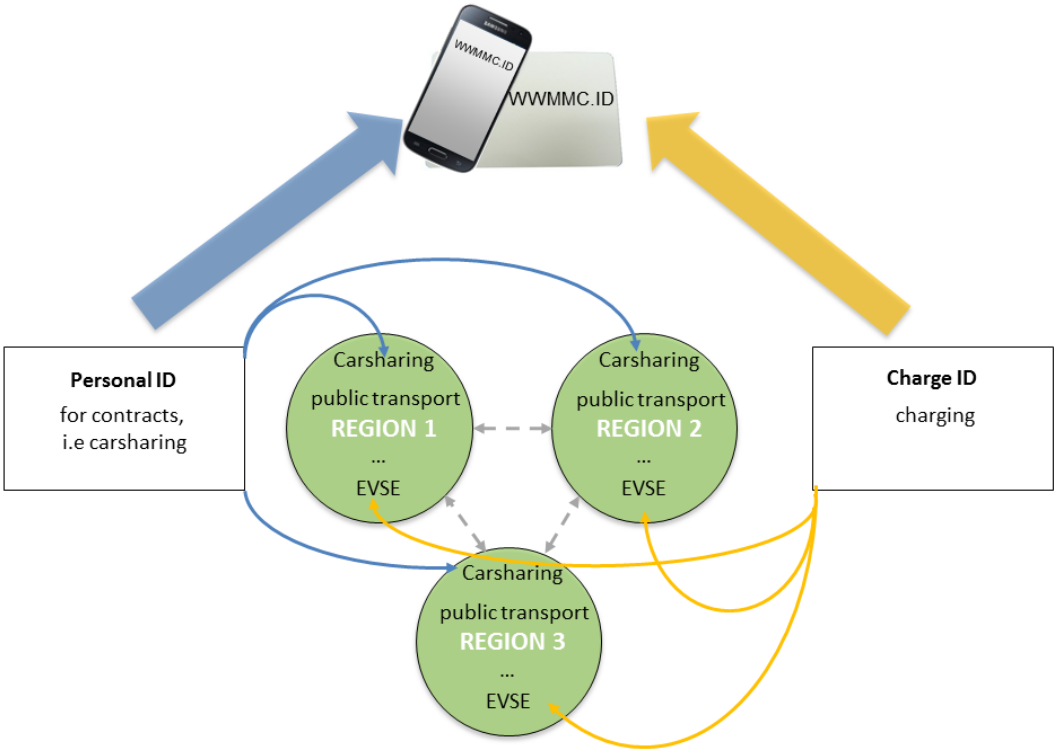

figure 1: personal ID and anonymous charge ID in the WMC+ network (Steffen Sklebitz)

The need for Identification: Selected Use Cases, Stakeholder and their Roles in the Business Processes of an E-Mobility Ecosystem (Markus Spiekermann)

Ration: Users to Vehicle	1:1	1 of many	Many to Many
Access to mobility	The user has a personal electric vehicle that he uses as he wishes	The user can make use of vehicles of a certain supplier, eg. a regional car club	The user shall make use of several vehicles from different providers. He is supposed to have seamless access to all kinds of mobility
Access to energy infrastructure	The electric vehicle needs to be charged more often. People in urban settings regularly don't have access to a fixed parking space	The infrastructure can be installed on the parking lot of the car club.	The user resp. the used vehicle needs access to energy, no matter where the vehicle is.
Conclusion			The access to energy infrastructure and mobility needs to be harmonized. Billing and clearing between the different providers is necessary to give the user a "hassle free" experience. *Interoperability* is the keyword in this context

Definition of the Rolls of E-Mobility Stakeholders (Frank Thurecht)

- Users: they use the vehicles
- Mobility Service Providers: offer means of transportation like car sharing, public transport
- Electric Mobility Service Providers: They order charging services from the chargepark operators and pay these. The EMSPs are the contract partners of the users.
- Energy Provider: They deliver the electric energy to operate the chargeparks
- Chargepark operators: They setup chargepoints and operate them. Chargepark operators are contract partners to clearinghouses. Chargepark operators deliver electric energy to the vehicles of the users.
- Clearing houses: they are responsible for data privacy and for the clearing of the services of the chargepark operators with the EMSPs
- ID-Provider: They create secure ID media, usually RFID-Cards but also smartphone apps and other means
- Technical service provider: The TSP offers the technical service to run the business cases of the Chargepark operators or the EMSPs. Usually multi client capable software as a Service Solutions are offered.

Sources

SPI 2012: "Nutzungskonzepte für Elektrofahrzeuge am Beispiel des CarSharings" - 17.Magdeburger Logistiktagung, Magdeburg, 14.06.2012, Germany

International RFID Charging Card Standard (Håkan Källberg)

The RFID technology was developed mainly for authentication purposes. Payment systems were one of the possible targets for the technology. As payment system is and probably should be a conservative sector, RFID seldom was used as payment authentication token, until now. As the completely new market field electric vehicle charging opens up it is a good opportunity to put RFID technology to real use.

Motivation for the Usage of RFID

RFID has many advantages, like cheep reader technology. It is completely contact free, hence the readers, can be well protected, behind a closed plate of e.g. plastic or glass.
The current RFID card technology can hold and quickly transfer large certificates, which was not quite the case with earlier models.

Suggested RFID Standard

The proposed standard for RFID card numbering is described in a document written by Johannes Bauer [1].

Card Identification Number: The RFID card is produced with an UID that gives the card it's unchangeable identity. The UID is machine readable. The card also needs a human readable identity, which shall be printed on the card. It will also be written into the card storage, signed together with the card UID and hence so be physically bound to the card. The signature and the card number can be read by the card reader.
There is a suggestion for an international standard for this card number, DIN Spec 91286 [2]. Goal is that the card number should be an address to the responsible registrar. It consists of the well known two letter ISO 3166-1 [3] country code, a dash as separator, a unique issuer alphanumeric code, a dash, a number given by the issuer, a dash and a final check sum.

DE-8XX-123456-X

There has been a confusing naming of this card number in the German standardization process. For historical reasons it has been called "contract ID", as the thinking at that time was, that one card should have a one to one relation to an energy contract.
This thinking would limit the flexible use of RFID cards. The RFID card is just a identification token, like any ID-card. We can choose to bind it to any contract we want, or it can be used without contract as e.g. an entrance card in a door.

It might be interesting for e.g. families or companies to register more than one card to the same charging contract. One payment, but the use can be individually monitored.
Nothing prohibits the use of the charging card for completely unrelated purposes, e.g. a sport center might bind the charging card to a membership contract. It could be used for payments and access in the sport center — completely independent of the use of the card by a charging pole. Everything needed to register the card for a new service is written unchangeable but machine readable to the card storage.
Although technically unimportant but therefore logically important we strongly disagree with the term "contract ID", found in German papers, for the number described above, as it limits the thinking around the card! We will just call it a "card ID". The card is an authentication token nothing more, nothing less.

Security: As mentioned above, the physical card UID together with the human readable card ID are joined together and digitally signed. All this is written to the card. In this way the UID and the card number are securely bound to each other for all times. The reader of the card might not know the signer, but this is not important. Someone has to be found that is taking responsibility for the card, the card issuer or someone he can refer to.
Card Issuer: Cards can be issued from any organization willing to follow the standard. Preferably mobility providers holding customer contracts are suitable. The card issuer organization has to require a national card issuer code from an authority or coordination organization. This three letter alphanumeric code is the second part of the card number.

International EVSE-ID Standard

For alternative authentication methods, e.g. for charge points lacking an RFID reader, you might contact your mobility provider and authenticate using a mobile application or a simple phone call. You have to be able to identify which charging point you want to activate.
There is also a standard proposal for unique numbering of charge points, DIN Spec 91286 [2]. As it is designed to be entered in a mobile phone, it is numeric. It consists of an operator code and a running number, which the operator can use freely. For international use it should be prefixed with the international telephone number prefix, like +49 or 0049 for Germany.
With this information it is possible for the card issuing mobility provider to put a charge order through the network of clearing houses finally opening the addressed charging point.

Distributed Market Relations

Customer Holder / Mobility Provider: The organizations that have got the contracts with end customers and the contract related RFID card data might be called *Electric Mobility Providers*, *e-Mobility Providers* or similar. They keep the connection between the card numbers and the related contracts. The personal data of the customer and bank data or similar are connected to the contract only.

Charge Park Operators: Charging points are grouped in charge parks, which can be parking places with one or more charge points. One or many charge parks may be operated by a charge park operator.

Clearing - Two Models:

At a charging point an RFID card is presented. The card is read and an *authentication request* is sent to the backend IT-system to which the chargepoint is connected. The backend might not handle customers and cards itself and can deliver the request to it's backend, holding customer data and card numbers. If the card number is available and actively connected to a running contract, an authorization to charge, a so called *charge order* is delivered back.
This works for customers belonging to the same infrastructure cloud. If the card and the owner of the card are not registered in the backend, the process of clearing the transaction starts.
There are two different models for handling the problem:

- The first is a regular clearinghouse.
  The backend, or even the charge point itself, depending on local structures, does not get an authorization back and hands the request over to a clearing house with which it has a contract relation. A clearing house acts as a sort of proxy, that finds the right way to the registrar of the card. But the clearing house does more, it takes over responsibility for the request and for the following payment of the later charging session.

- The second model is a service that proposes a redirect of the request. It still has to have a contract relation with both parties and tell the parties that this is the case. But it does not carry on the transaction. It does not perform payments.

<u>Clearinghouses</u>
The clearinghouse model takes complete responsibility for the performance of the transaction:
Contract Administration: The clearinghouse maintains contracts with it's parties. The charge park operator needs to know that he gets paid if he will accept to charge a car, even if the RFID card is not locally known.
Chains of Trust: As a clearing house gets a charge request, it might be clear where the owner of the card id can be found. In all other cases e.g. with international clearing, another clearing house might know more about the holder of the card. It is no problem, the first clearing house asked with the authentication request hands it over to the second.
Even this house might handle the transaction over to another clearing house. Finally the card holder will be found, and he can safely issue a charge order, knowing that it is his customer, identified by the credentials on the card. The end parties do not know the

complete road of the transaction, just their local next hop. This is called a chain of trust, and has to be supported by contracts.

Recursive Contracts: In a trust chain the participants only have got a contract with their local partner. They have to know, that if the request is handed over to another clearing house, a similar contract has to exist, which states that the next clearing house takes responsibility for the transaction and the payment. This is called a recursive contract. In this way transactions can be legally bound to a contract the whole way although the participating parties don't have a relation to more than the closest one in the chain. This works well, also over national borders and continents.

Handling of Currencies: As transaction crosses borders a currency conversion has to take place for invoicing and/or payment. Currency risks are involved because the exchange rate can vary between the delivery time and payment time. These risks and extra handling can be comfortably covered by the clearing houses.

Regulatory Handling of Energy Trading: Today trading of energy is differently regulated and restricted in different countries. To create an open marketplace for electric vehicle charging, many of these local restriction have to be changed. The clearinghouses, with their legal expertise will be central players trying to achieve this open market where transactions easily can be cleared between countries.

Handling of VAT: Although invoices cross borders, local VAT has to be paid, as the product basically is consumed locally. The VAT roles may vary from country to country. EU is a special case with special roles. There might be refunding processes for VAT between countries.

All this requirements can be solved transparently to the to trading parties by a clearing house.

Costs of a Clearing House: Technically a very low overhead is needed to run a clearing house handling transactions. Administratively, contracts have to be written and managed. Handling of money transaction including payment and currency risks as well as tax issues is substantial work and has to be payed with roaming fees and fix contract holding fees.

The clearing house may anyway reduce costs for the end parties through bundling of payments into one invoice per payment period.

<u>Direct Lookup / Information Center</u>

An alternative model, would be an information infrastructure retrieving and offering data in a way that the parties are enabled to communicate directly with each other. This model requires the same contract infrastructure as above, but no money transactions are performed. They are left to the end parties to handle as they want.

Lets call this model "*Information Centers*". The contract parties find the two end points for the transactions, possibly over many steps. They deliver contact information to the end points, including a signed token that states that both parties stand under contract and safely can put orders and require payments from each other.

This might be a good alternative especially for domestic transactions where no extra complications are involved. To our knowledge nobody is working on such a model today, but

we see it as an alternative, that can coexist with a traditional clearing house model. An end customer might choose a traditional clearinghouse for international transaction to be relieved from currency and legal complexity, and an information center for a domestic transaction, where the conditions are well known.

Communication Protocols

The protocols used to communicate between entities are not the main scope of this article. There are already some suggested standards, but they do still need to evolve somewhat.
Technically it is quite clear that the communication will go over common web services protocols, because their common availability. The security issues are also well understood.
Commonly the communication standard SOAP is the suggested application layer above the web services transport layer. We are arguing against SOAP, because it is definitely unnecessary complex and has a big data overhead. The different implementations of SOAP are not known to be very compatible to each other in detail, although they claim to follow the standard. SOAP is hardly evolving any more.
As the volume of data that needs to be transmitted is very low, we suggest to use the substantially compactor protocol *REST* transmitting *JSON* documents. It is important that the transaction works quickly over the many involved steps, otherwise the acceptance of the payment method will be low. We have been able to prove that transactions over many REST steps, can work quickly enough to feel close to instant. This is not the case with other commonly available card payment systems used today. The use of SOAP would also work against these goals.
Regulators may require signed messages, which will produce some overhead. It is technically not quite necessary, as the transactions run between partners under contract and trough (TLS) encrypted channels.

Conclusion

If the international EV charging stakeholders can agree on these, or similar international standards of the RFID card, its Card-ID number, EVSE-IDs, communication protocols and contract infrastructure, we will get an open and flexible EV charging market that can evolve and grow over many years.
The main advantage is, that this model requires a bare minimum of technical overhead and central organizations. It is completely distributed and not restricted by patents and intellectual properties. It allows a free evolution of the market.
Still regulations and numbering authorities are not in place, but it is basically clear what needs to be done.

References

[1] Technische Spezifikation der RFID-Umgebung zur interoperablen Authentifizierung v1.0 Johannes Bauer, Bosch Software Information GmbH 6. June 2011
[2] DIN Spec 91286 Contract Id and Electric Vehicle Supply Equipment Id November 2011
[3] ISO 3166-1 http://www.iso.org/iso/country codes

Secure identities (Willi Gramberg)

Today the problem of many business cases is that they must be user-friendly. On the other hand the identification of persons shall be unambiguous. Other objectives come into play here too. For example, while advertising companies want to have as much information as possible, customers usually try to avoid giving them private information.
Some business cases must also identify persons' legal status". Global mobility makes it necessary to have a smart look at the different characteristics of identity and designated roles.

Definition of Identity

Today in standard eBusiness environments personal data is asked in forms in an internet browser and the user can select a username and a password to get access to his data and business cases. In all these cases the personal data given to a corporation depends on the will of the user. On the other hand the identity is not controlled against a respected authority.
Also in many cases it is not really necessary to give one's entire personal data to a corporation. In addition, anonymous registration should also be possible in these cases.

- In some cases only the age is needed (f. e. to order a game restricted to persons over 18)
- he address has to be a real address (for delivery)
- personal data has to be granted through an authority (f. e. to rent a car
- anonymous registration (f. e. during charging)

So a system is needed that allows scalable identities to fulfill different roles.
An example is traveling using different mobility forms:

- A train for the long distances
    - information on mileage is needed
    - Information for billing is needed
    - Personal identification is no necessary
- An electronic car for use in the local environment
    - Information on positioning is needed
    - Information on mileage is needed
    - Information for billing is needed
    - Personal identification is necessary
- Charging the car
    - Information for billing is needed

- Information of charged energy is needed

Data privacy protection

Today customers look in detail at which data they give to companies and they wish to control what exactly is done with this data. So many users are not willing to give their real data to corporations and many fake accounts exist.
Also actually the main system to re-identify customers is a system where user ID and password is used. This system gives only poor security and forces users to use long and not easily remembered passwords. This system is called one-factor authorization.
A modern system should follow the premises acceptance without discrimination and take account of the following factors at least:

- Data minimization so that there is no need to operate with more data than really needed for the actual process
- Protection of user data
- Secure authentication of users

Secure Solution with secure personal identity

The secure personal identity solution from OpenLimit SignCubes offers a solution for all these challenges. With secure personal identity it is possible to separate the identification of a user from the offered services. This will be done with trusted concepts using certificates.

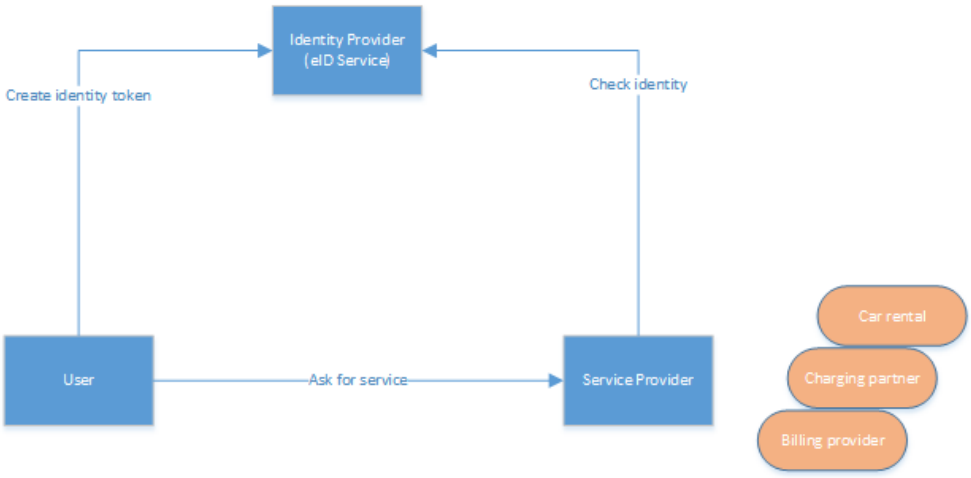

figure 2: triangle of trust (Willi Gramberg)

- Identification against an accepted authority
  - National ID card

    - DE mail (Germany)
    - Authorized identification service (eID service)
- Two factor authorization with a token (mobile phone, electronic card
    - Gives user the possibility to decide and check which data is given
    - Easy to use
    - Integration with signature services possible

The secure personal identity solution guarantees privacy by design on one site and also guarantees the identity of users against business partners.

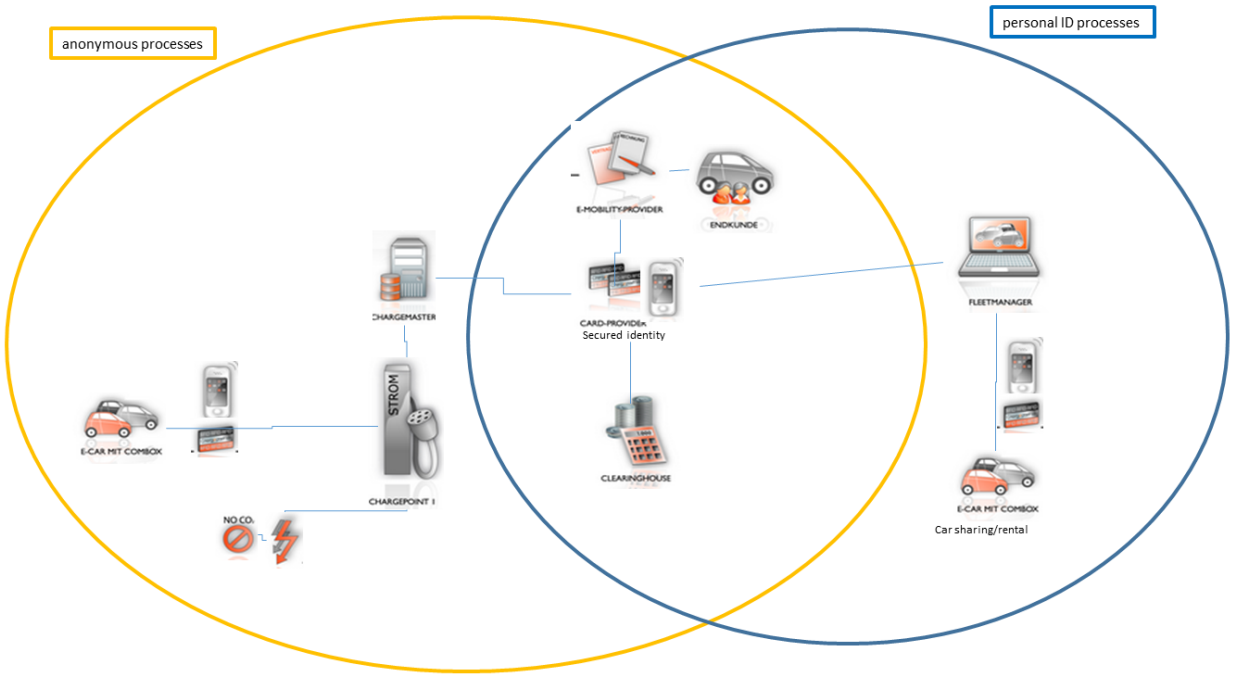

figure 3: Circles of needed identity (Willi Gramberg)

The three scenarios displayed in chapter above would be supported like this:

- A train for the long distances
    - At start of trip the user buys a ticket online using his secure personal identity profile. This profile guarantees the train company that this person is real and solvent.
    - Starting position is stored at the train company
    - At the end of this part a message is sent to the train company together with the position and the secure personal identity profile for train
    - The train company sends a debit order to the billing company together with an identification of the user but not the start and end positions
    - For all this transaction it is not necessary to have full personal data as the identity of the user is granted through the identity provider
- Renting an electronic car for use in the local environment
    - At start of trip the user reserves a car online using his secure personal

identity profile. This profile guarantees the car rental company that this person is real, solvent and has an actual drivers license.
    - Starting position is stored at the car rental company
    - At the end of this part a message is sent to the car rental company together with the position and the secure personal identity profile for car rental
    - The car rental company sends a debit order to the billing company together with an identification of the user but not the start and end positions
    - For all this transaction it is necessary to have full personal data as the identity of the user is granted through the identity provider. This data is needed to check the driver license and to have a contact person in case of an accident.
- Charging the car
    - The driver starts charging the car and identifies himself with his secure personal identity profile for charging. This profile guarantees the charging company that this person is solvent. For this action it is not necessary to know that this card belongs to a person also an organisation can be the holder of a card.
    - At the end of charging a message is sent to the charging company together with the number of kilowatts and the secure personal identity ID for charging
    - The charging company sends a debit order to the billing company together with an identification of the user without positions.

To use such a secure personal identity profile it is only necessary to be registered once time by an accepted identity provider. This could be a car sharing company, a post office with an extended post ident process or another office accepted by several organizations. Here the identity of the user is checked and an ID is generated. This can be generated on a mobile phone, a smart card or an USB token. It is also possible to deflect this identity from a national ID card like the German ID card.

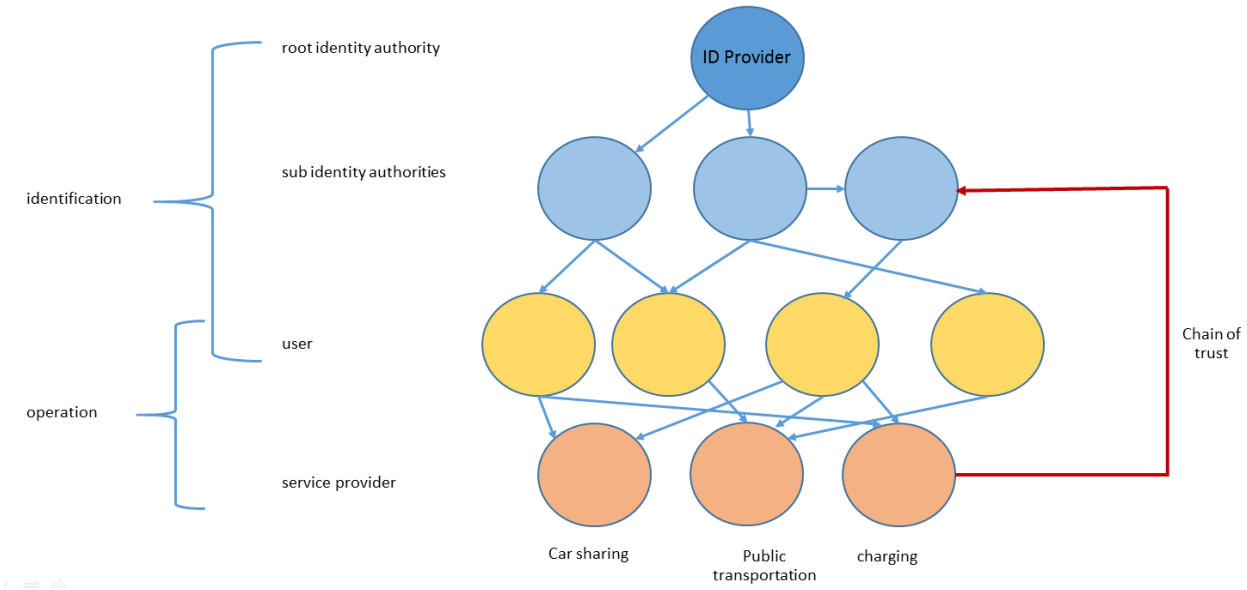

figure 4: Hierarchy of trust (Willi Gramberg)

The process of secured personal identity follows several technical guidelines from the German BSI (Federal office for information security). These are the leading guidelines for such themes. The most important guideline for this complex are:

- Technical Guideline TR-03124 - eID-Clien
- Technical Guideline TR-03130 –eID-Server Version 2.
- Technical Guideline TR-03128 – EAC PKI'n für den elektronischen Personalausweis (EAC-PKI for the electronic ID card)
- Technical Guideline TR-03126 – sicherer RFID-Einsatz (TR RFID)

It uses similar technics as the german national ID card which is CC certified with EAL4+.

If the international EV charging stakeholders can agree on these, or similar international standards of the RFID card, its Card-ID number, EVSE-IDs, communication protocols and contract infrastructure, we will get an open and flexible EV charging market that can evolve and grow over many years.

Conclusion and further development

The main advantage is, that this model requires a bare minimum of technical overhead and central organizations. It is completely distributed and not restricted by patents and intellectual properties. It allows a free evolution of the market.
Still regulations and numbering authorities are not in place, but it is basically clear what needs to be done.

Apendix

Glossary

BEV	Battery Electric Vehicle
BSI	Bundesamt für Sicherheit in der Informationstechnik
EVSE	Electric Vehicle support Equipment
NFC	Near Field Communication
PHEV	Plugin Hybrid Electric Vehicle
RFID	Radio Frequency Identification