DIGITAL WALLET AS A FOCUS FOR W3C STANDARDIZATION

Jörg Heuer, Oct 2014

W3C PAYMENT IG

Day 1 - Input

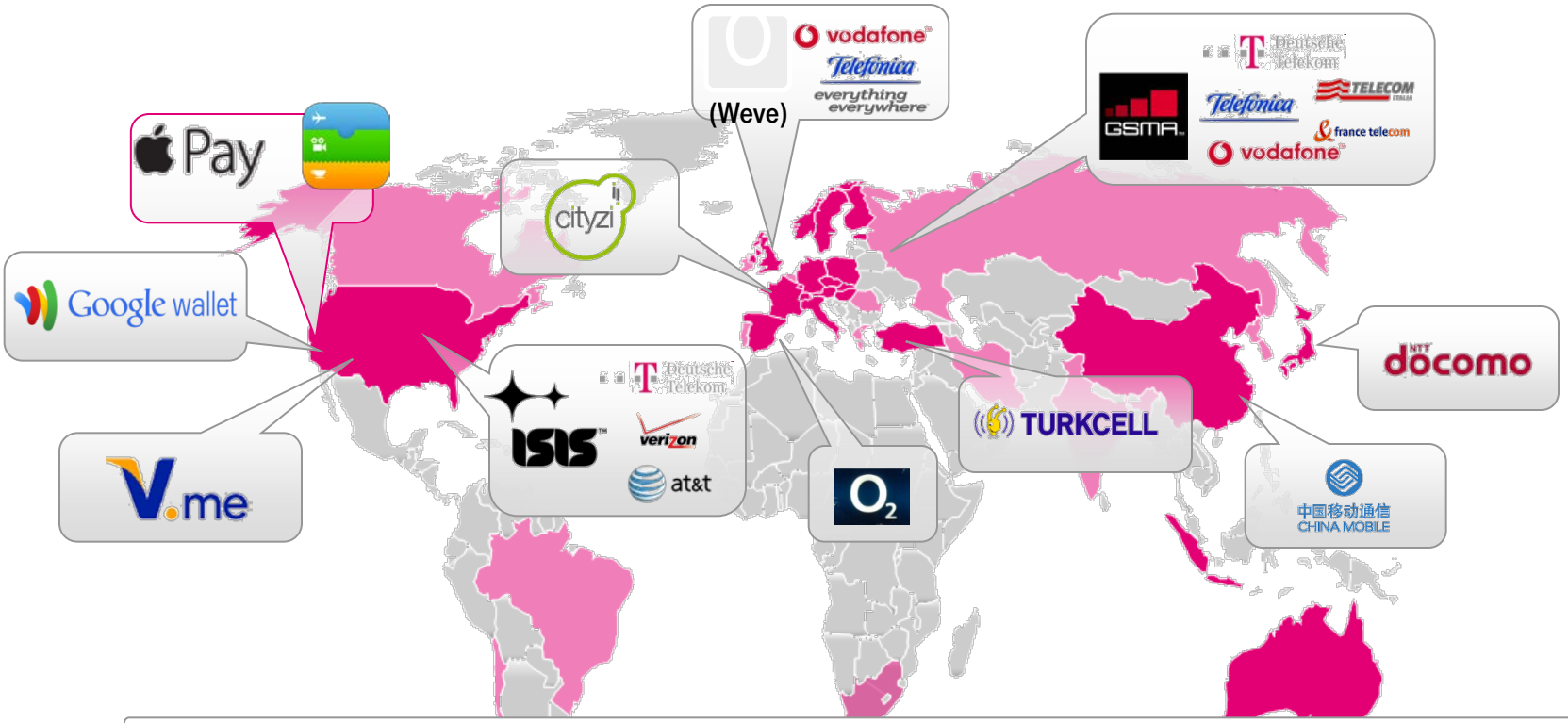
- Overview
- Our aspiration
- Our approach
- Demo

Day 2 – Proposal and Discussion

- Proposal
- Vision
- Working mode

MARKET OVERVIEW

MANY HAVE FOCUSED ON MOBILE WALLETS FIRST



"NFC a Mega-Scale Opportunity"

Google's CEO, 2011

…"vast potential in the mobile-payment market"…

VISA's CEO, 2012

"The opportunity for the wallet upwards of $400 billion"…

Placecast's CEO, 2012

…the smartphone will become a mobile wallet…

DT's Executive, 2012

…unprecedented opportunity…

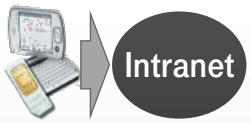
ISIS's CEO, 2012

Strong mWallet initiatives | Emerging mWallet initiatives | No initiatives known

T-LABS' WALLET DEVELOPMENT HISTORY

A CROSS-OVER OF NFC, SIM AND INFO CARDS

Prepping up Technologies | **Early Mobile Wallet** | **Convergent Wallet** | **Wallet Ecosystem**



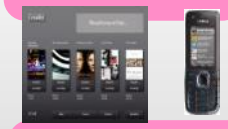
UICC-secured VPN

P2P money transfer

NFC & UICC-based facility access

InfoCard

Wallet UI and card metaphor on iPhone



Mobile Wallet for NFC-based POS payment

Online shopping on PC using mWallet and NFC for payment

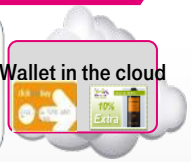
Online payment

mWallet for payment, loyalty cards and coupons

Issuer portal for coupons

GSMA POS Protocol

Issuer portal



3rd Party App Protocol

2006 | **2007** | **2011** | **2012** | **2013**

Public Transportation
- Project RMV2go
- German eTicketing Standard VDV KA
- NFC Handset (J2ME)

NFC Trial @Telekom Cafeteria
- POS Payment
- Integration of XTC Platform
- Collection of Bonus Points
- NFC Handset (J2ME)

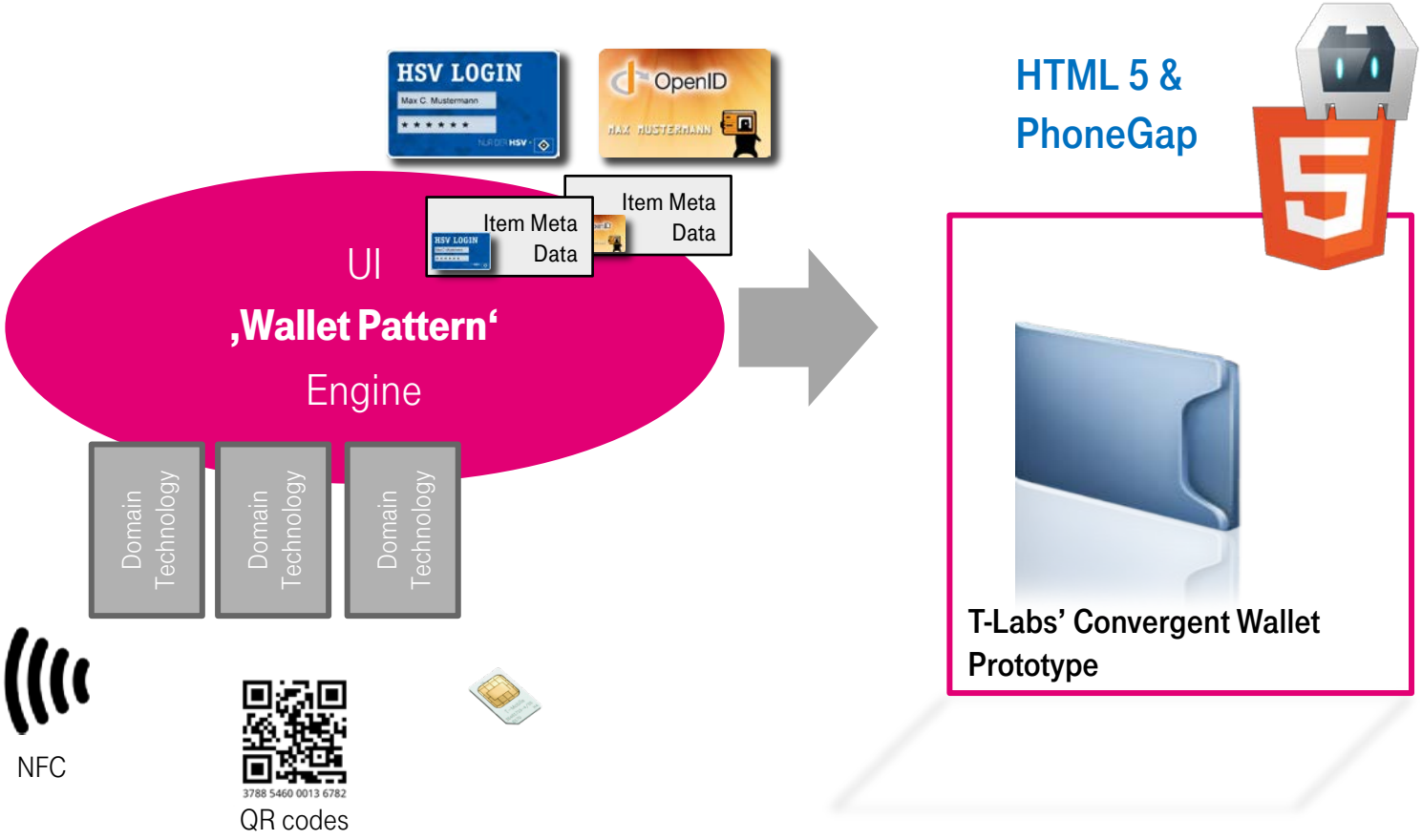
MWC & CeBIT 2011
- POS Payment
- Public Transportation
- Event Ticketing
- iPhone/NFC Handset (J2ME)

IAA 2011
- Car Key in mWallet
- Continental, T-Systems
- Online Payment
- NFC Handset (Android)

CeBIT 2012
- POS Payment
- Issuer Portal
- Loyalty, Couponing
- NFC Handset (Android)

2013
- HSV Trial
- MWC: Future Wallet
- CeBIT: Future Wallet

FROM A GENERIC USAGE PATTERN A PROTOTYPE WAS IMPLEMENTED…



… AND WE WERE ABLE TO DO IT IN HTML 5 WITH CORDOVA!

VISION

A tool for users where all types of credentials are stored; with appropriate security; for use in all kinds of personal digital transactions; in a vivid ecosystem– always under the control of the user on his trustable device/ service.

What can be our impact?

- Increase security of identity, payment and eCommerce transactions with crypto and security hardware if available
- Give users maximum control over their entitlements, identity data and foster privacy through support of multiple identities (pseudonyms)
- Avoid silos governed by browser, OS, device manufacturer, security means or service provider
- Secure interoperability between wallets, contents in the wallet and technologies of the underlying systems
- Create roles for trusted parties, attractive brands in digital services (**wallet providers, wallet operators, security providers**, issuers, services, ...)
- Serve as level playing field for innovation in payment, security, marketing and privacy

T-LABS AT W3C
OUR PROTOTYPE AND LESSONS LEARNED

- Experimentation and collaboration with various companies has shown, we can achieve much more than expected; academia, politics and privacy experts encouraged our work
- Starting 2013 we were able to implement a prototypical wallet framework using HTML5 and Cordova
- Central concept: Wallet and Items
- We developed the understanding that most of the solutions must come from outside
- Many interfaces are lacking, many questions are open
- Proposal to work out a joint vision and prepare use cases in W3C task force

A CONVERGENT DIGITAL WALLET CAN LEAD USER-ORIENTED TRANSACTIONS INTO THE FUTURE

Payment

- unifying proximity and online payment
- avoid storing critical information at shops/ services

eCommerce

- Omni-channel commerce
- Storing and using payment and loyalty, cards, coupons the same way – online and offline

Media

- Personalization at home and on the move
- Behind a ‚paywall', or some kind of DRM

Smart Homes/ Cities

- The user's agent to securely interact with an increasingly digitized environment

A push for a user-centric digitalization of our world

POSSIBLE BENEFITS OF A DIGITAL WALLET
FOR THE USER

- Transparency – no pre-configured payment cards in some online service stored somewhere
- User control – every transaction flows through his wallet, the user decides and authorizes
- Convenience – every relationship to a vendor, every account is represented
- Openness – every bank, vendor, issuer, or service provider can issue wallet items – even the user
- Security – virtualized (hardware) tokens instead of username/ password
- Privacy – use of pseudonyms is eased, framework might support ‚certification for untrackability‘
- Anonymity – transactions can be made without the use of trackable and replayable numbers. etc.

POSSIBLE BENEFITS OF A DIGITAL WALLET
FOR THE ECOSYSTEM PLAYERS

- Open ecosystem – everybody can create their own wallets and their own wallet items
- Cost efficient – finally hardware-backed security becomes affordable to a wide range of uses
- Attractive to brands – the brand is always recognized
- eCommerce – covers a wide range of eCommerce cases, increases take-up and efficiency
- Merchants are able to pursue ‚Omni Channel Solutions' in a standardized ecosystem
- Legacy support – optical systems like bar code and QR, TAN, and others
- Technology agnostic – open for new communication and security technologies
- Grounded – fits into existing ‚physical' processes, but guides towards digitalization
- SE/ SIM (and TPM?) – hardware capabilities can be offered in an open market

T-LABS' WALLET

ALL THE SCENARIOS – IN ONE SOLUTION?

A COUPLE OF STANDALONE PROTOTYPES NEEDED UNIFICATION

UICC-secured VPN

NFC & UICC-based facility access

NFC Cafeteria Payment

Online shopping on PC using mWallet and NFC for payment

mWallet for payment, loyalty cards and coupons

GSMA POS Protocol

3rd Party App Protocol

InfoCard

P2P money transfer

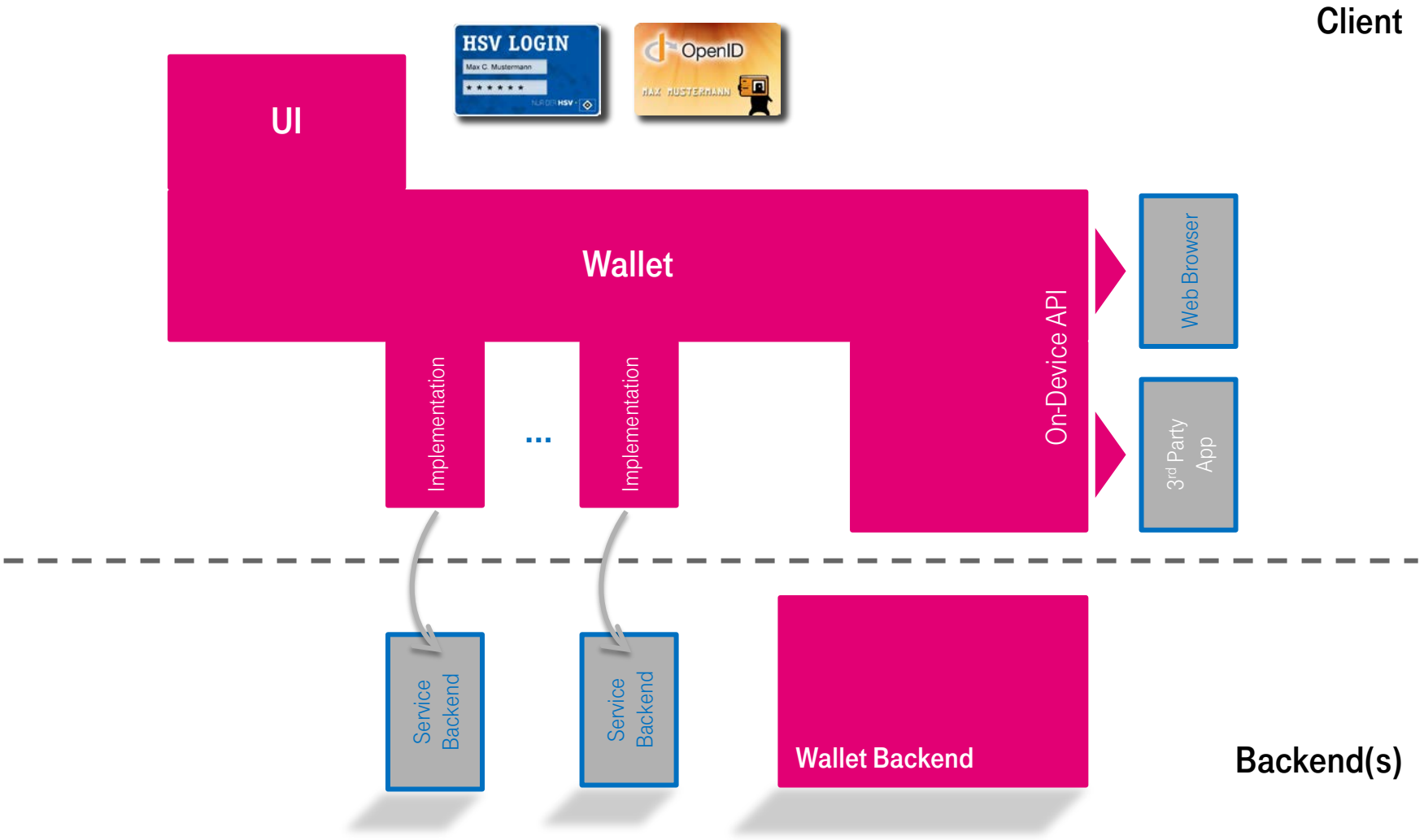
NFC Ticketing

Mobile Wallet for NFC-based POS payment

Online payment

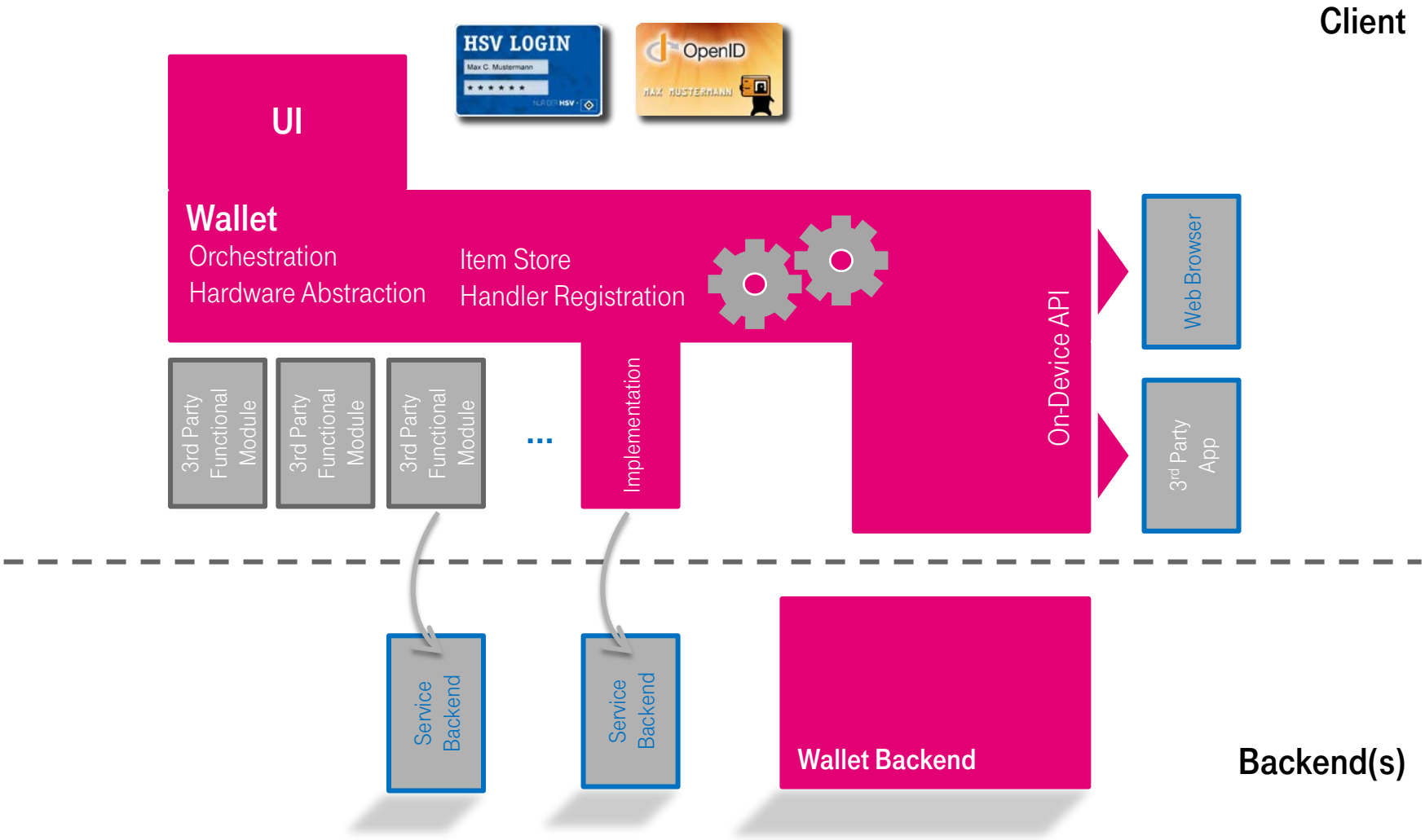
Issuer portal for coupons

T-LABS' CORE WALLET
OUTLINING THE FUNCTIONAL SCOPE



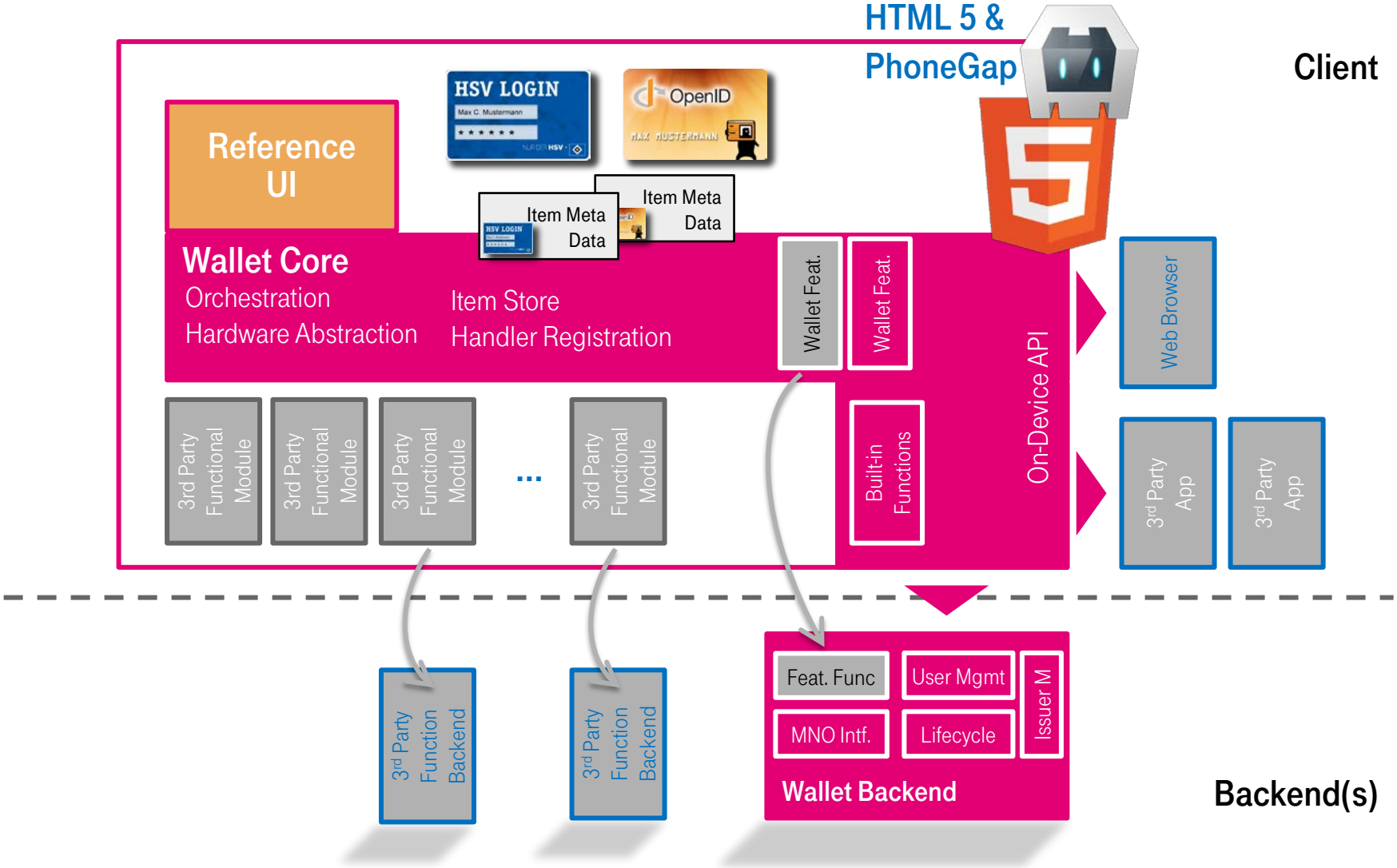
T-LABS' CORE WALLET

LAYING OUT THE 'ENGINE' AND OVERALL ARCHITECTURE



T-LABS' CORE WALLET

IT CAN BE DONE IN HTML5!



A SIMPLIFIED FUNCTIONAL VIEW

ITEMS ON A PLATFORM MEDIATING TECHNOLOGY

REFERENCES
IMPORTANT WORK TO LOOK AT

GSMA

- Wallet white paper put out by GSMA
- POS VAS protocol recommendation put out by GSMA (demoed at MWC 2014)
- Wallet on-device API introduced (and implemented)

Mozilla

- T-Labs have been instrumental in developing the NFC/ SE stack for FireFoxOS
- Perhaps, they'd like to take custody of a reference implementation?

Privacy

- Appointed ‚Ambassador for Privacy by Design' for the convergent wallet concept

Proof of Concept

- Run essentially the same code on Android and iOS (w/o SE/ NFC yet)
- Authenticate to PC with mobile phone via NFC/ via optical, receive a ticket
- Login to web page on same device with wallet, get a club card using a secure element

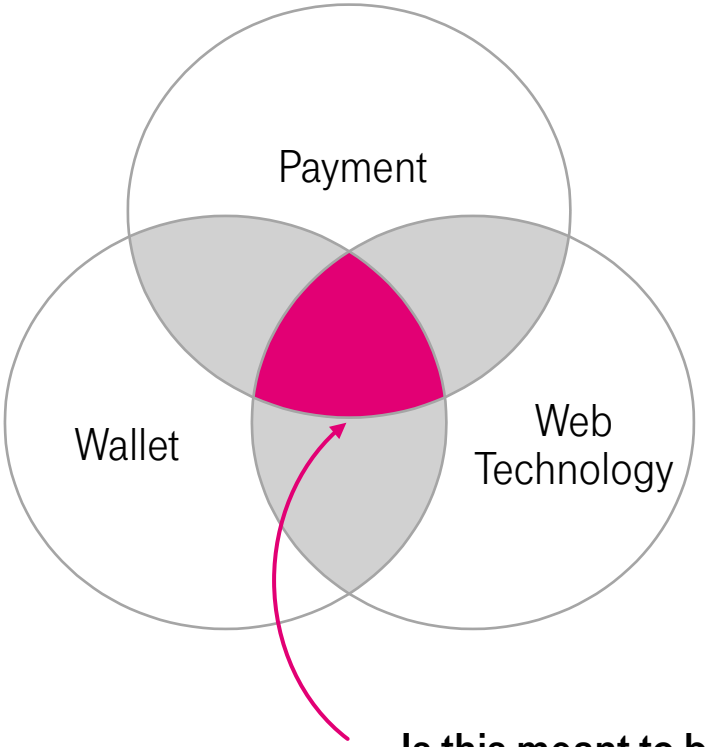
A push for a user-centric digitalization of our world

DAY 2

W3C PAYMENT IG
PROPOSAL

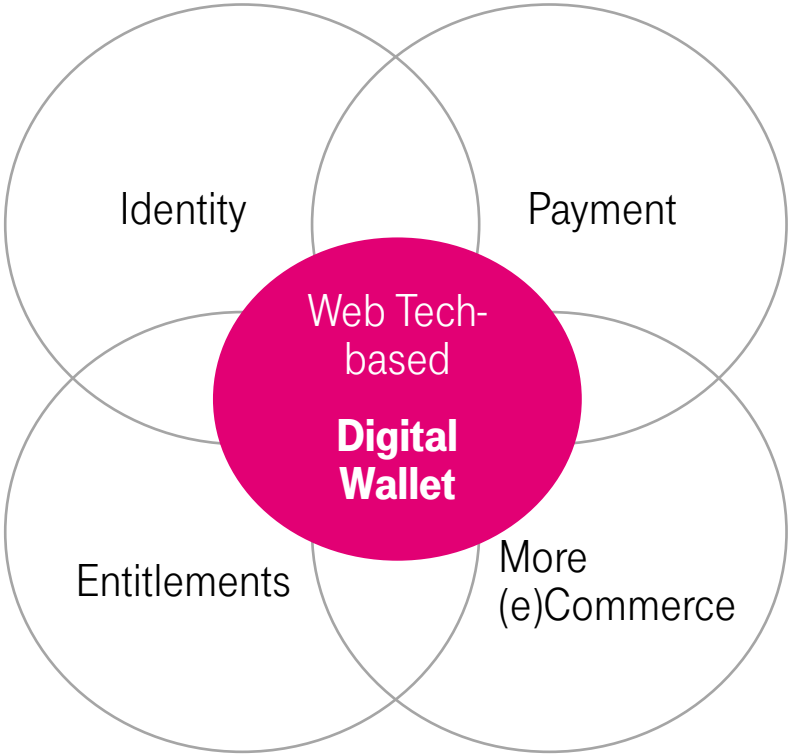
- Discussion on concepts, ideas, and demos of day 1
- Create a task force to take on the creation of
  - a joint vision
  - use cases
- Alternative ideas for conduct?
- Work on focus and organization (if any agreed upon)

FOCUS ON PAYMENT, WALLET, WEB
ALL AT THE SAME TIME (PROBABLY DOESN'T WORK)



Is this meant to be our focus?
(...and what about identity, coupons, tickets...?)

FOCUS ON WHAT CAN BE DONE WITH W3C'S TECHNOLOGY
SETTING THE FOCUS

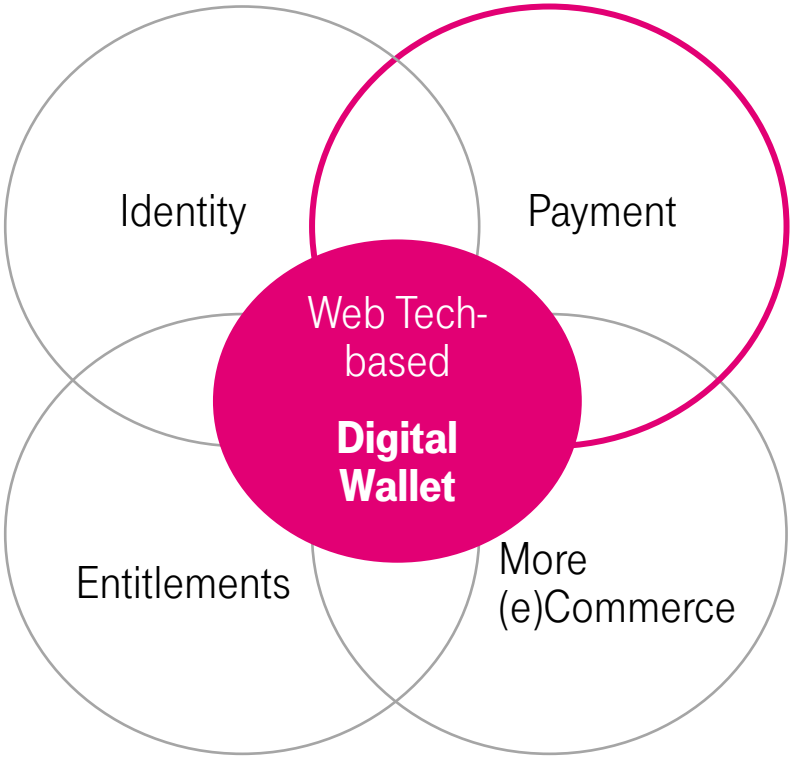


Wallet as a Paradigm

- Item-based
- User-centric
- Proximity – online convergent
- Technology-agnostic
  - wrt/ communication
  - wrt/ security
- Business-model agnostic
- Enhancing user-control and privacy

PROPOSED FOCUS FOR A START

PAYMENT THROUGH THE DIGITAL WALLET FOR A START



Open Issues

- Regard wallet as a ‚Black box', not a solution
- Add more insights and ideas
- Derive requirements
- Identify interfaces to be standardized
- Identify need for data format standards
- Check with other organizations/ standards bodies

- T-Labs offers their proof of concept as ‚straw man' and basis for demos

UP FOR DISCUSSION
OPPOSITES ATTRACT 1/2

Use vs. Register

- Terms like ‚identity' and ‚authentication' are used in different contexts
- They mean different things when registering for a bank account than for accessing the account statement
- People may ‚use' content from a wallet every day, to register, however, other instruments may be required; both cases need to be differentiated

Hardware vs. Software Security

- Authentication can benefit from hardware like SEs, TPM, etc. being available
- Some processes can be traced back to issuers – aka ‚risk manager' – replacing hardware tokens as we are used to (Android HCE, tokenization, etc.)
- In many cases, cryptographic keys in main memory would already be a big step forwards (compared to username/ password e.g.) and more appropriate in pricing

Client-centric vs. Cloud-enabled

- A wallet with all its content on a device has benefits: mobile devices can be carried around, on-board security hardware is available for strong authentication
- A wallet in the cloud has its benefit: wherever there is a web browser, you can use it
- Web technology running on offline devices as well as in a browser does the trick

UP FOR DISCUSSION
OPPOSITES ATTRACT 2/2

Proximity vs. Web

- The physical world demands for a plethora of special technologies (NFC, optical codes, Bluetooth LE, ...)
- The web could unify transactions for payment, identity, authentication, etc. – but hasn‘t achieved too much so far
- Convergence is a business driver promising convenience and less media breaks

Payment vs. Non-Payment

- Merchants and POS-people see coupons and loyalty cards as part of the payment process
- Financial institutions see all transfers, charges and exchange rates too, but aren’t interested in coupons and such
- The user‘s expects security, transparency, openness and convenience

We believe that all these seeming opposites can be fulfilled within one concept; cutting across many domains and opening up interfaces we should be able to come up with a harmonized user experience according to ‘wallet pattern’ flexible enough to be adopted to various industry’s needs as well as cultural and legal differences.

W3C PAYMENT IG
PROPOSAL

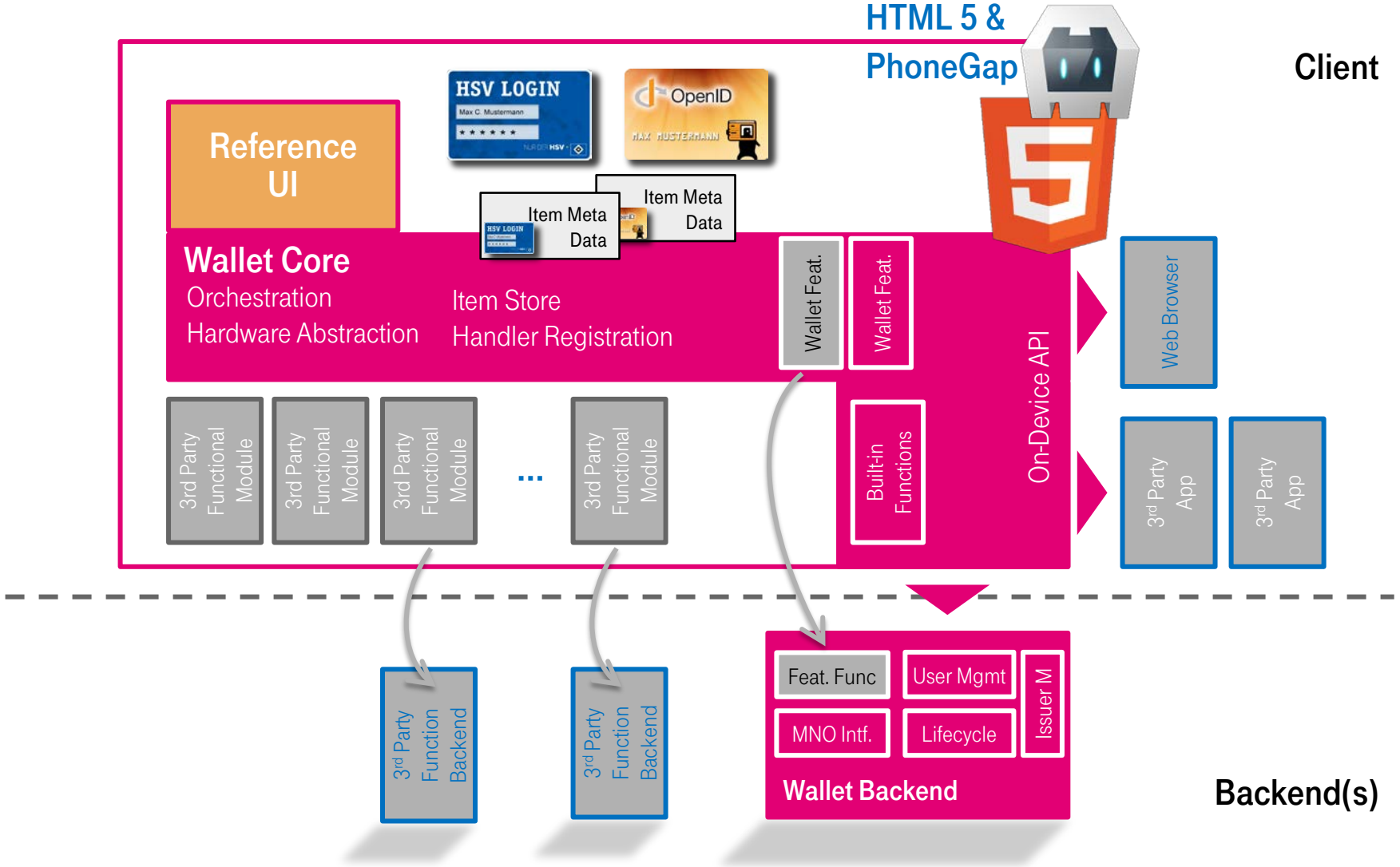
- Discussion on concepts, ideas, and demos of day 1

- Create a task force to take on the creation of
  - a joint vision
  - use cases
- Alternative ideas for conduct?
- Work on focus and organization (if any agreed upon)

T-LABS' WALLET AS A CASE STUDY

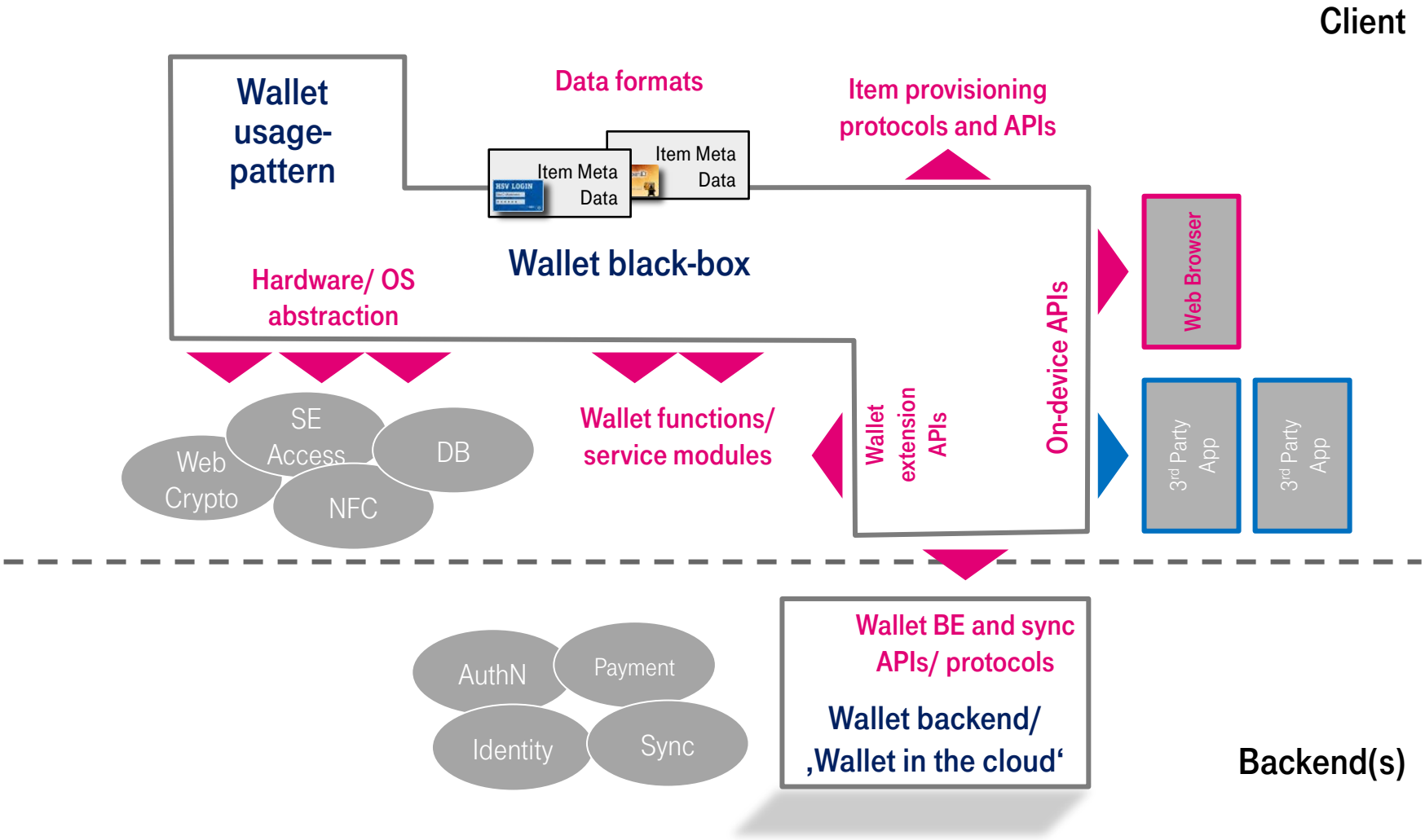
T-LABS' WALLET ARCHITECTURE

IT CAN BE DONE IN HTML5!



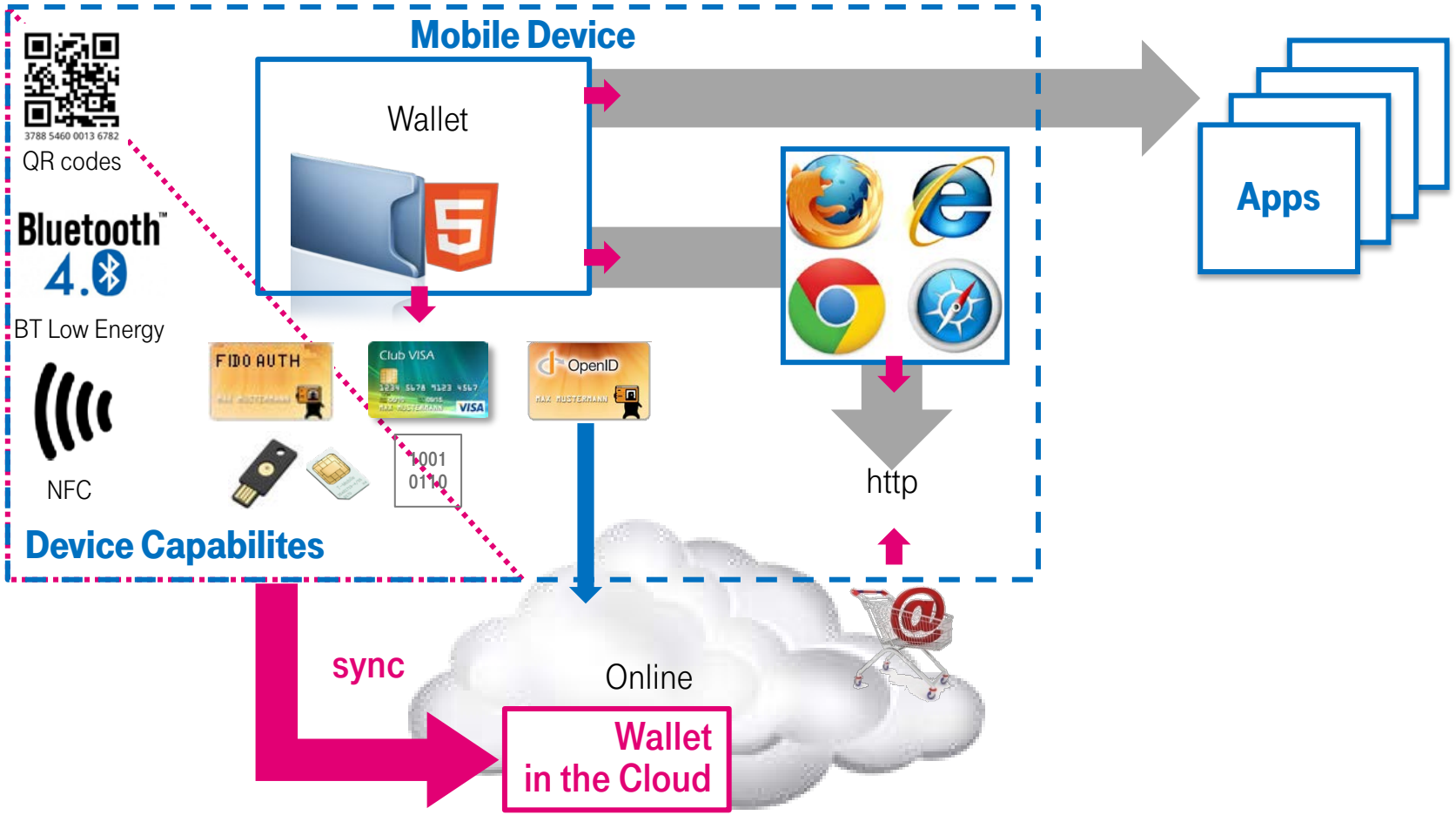
USING T-LABS WALLET AS A STRAW MAN

WHAT ARE THE INTERFACES, PROTOCOLS, DATA FORMATS?



BACKUP

AN ABSTRACT VIEW ON A WEB TECHNOLOGY-BASED WALLET FOR THE VIRTUAL – AND THE REAL WORLD



MULTI-PLATFORM AND ADAPTABLE

RUN EVERYWHERE, USE WHAT YOU FIND THERE

HTML 5 &
PhoneGap

=

Any Browser

Online

PATTERNS FOR THE MOBILE WALLET ADOPTED FROM KIM CAMERON'S LAWS OF IDENTITY

1) User Control and Consent

- Technical identity systems must only reveal information identifying a user with the user's consent.

2) Minimal Disclosure for a Constrained Use

- The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.

3) Justifiable Parties

- Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.

4) Directed Identity

- A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

5) Pluralism of Operators and Technologies

- A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.

6) Human Integration

- The universal identity meta system must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.

7) Consistent Experience Across Contexts

- The unifying identity meta system must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.