SIEMENS

Siemens Corporate Technology | June 2014

W3C Workshop on the Web-of-Things | Berlin | June 25-26, 2014

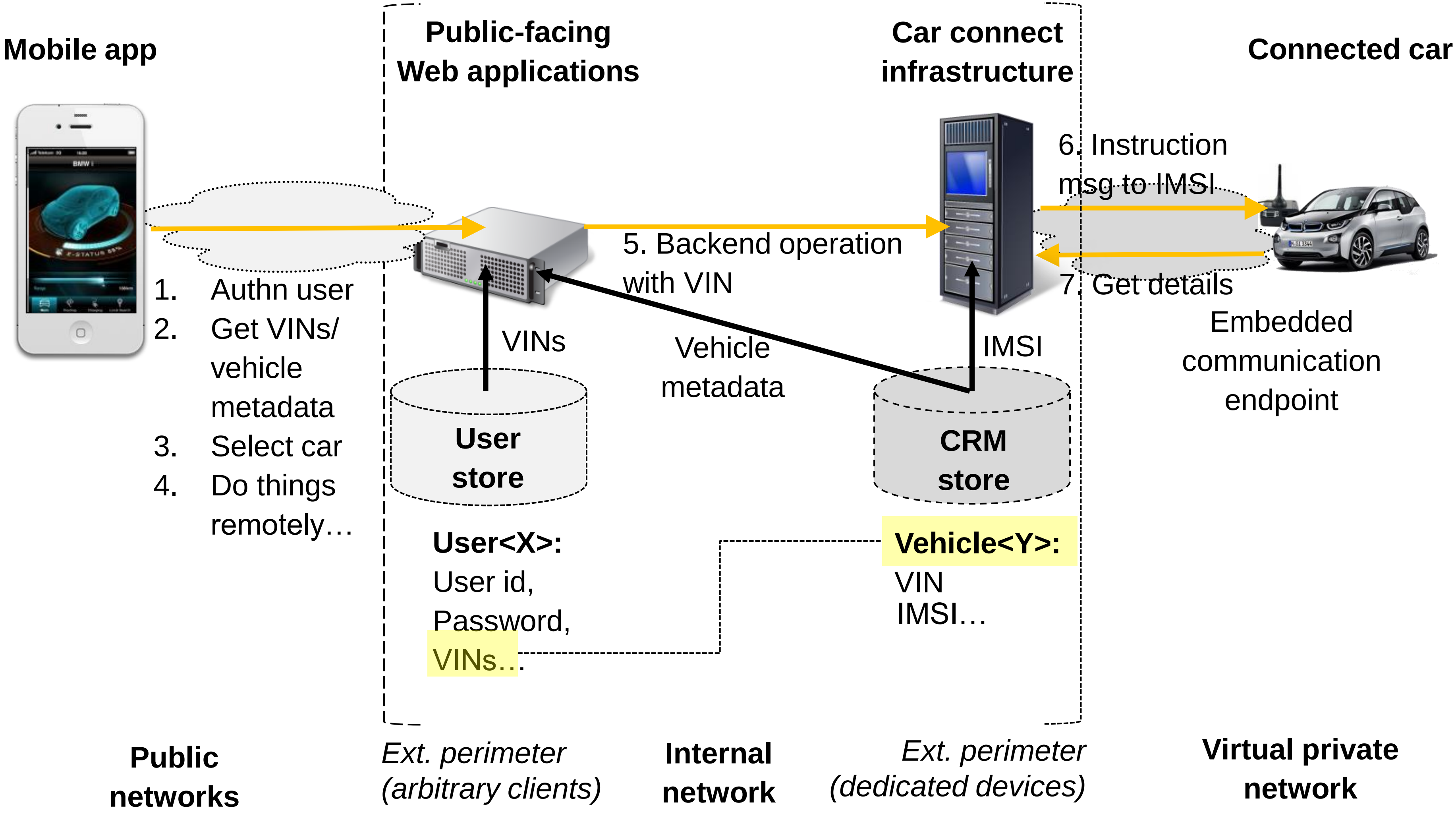
Authentication for the Web-of-Things

Oliver Pfaff

Why Am I Here?

- Buy a Siemens product → get a **distributed IT-system** or part thereof
  - *Today*: true for the majority of products
  - *Tomorrow*: growing share
- Siemens products handle **valuable resp. sensitive resources**
  - Corporate or private property
  - Critical infrastructure
  - Health information….
- Old school solutions in “*We Don’t Check Individual Objects–Because We Control Premises*”-style approach end-of-life → need to **assess individual requests and messages**
  - Authentication (*who sent this information, is it unaltered?*) presents a vital part of such assessments

Does a Best Practice Exist?



Mobile app

Public-facing Web applications

Car connect infrastructure

Connected car

1. Authn user
2. Get VINs/ vehicle metadata
3. Select car
4. Do things remotely…

5. Backend operation with VIN

6. Instruction msg to IMSI

7. Get details

VINs

Vehicle metadata

IMSI

Embedded communication endpoint

User store

CRM store

User<X>:
User id,
Password,
VINs…

Vehicle<Y>:
VIN
IMSI…

Public networks

Ext. perimeter (arbitrary clients)

Internal network

Ext. perimeter (dedicated devices)

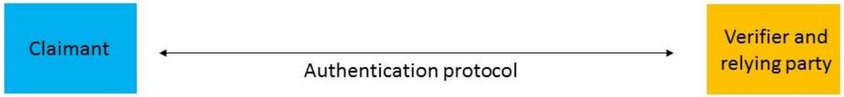
Virtual private network

Does It Provide an Overall Solution?

- The *connected car* use case is already **real**. The solutions use some **tricks**:
  - **Layered architecture**: user agents call public-facing Web applications, not the car connect infrastructure or a connected car
    - Certain CRM information is not revealed to public facing Web applications and mobile apps – for instance IMSI numbers
    - The fact that the service is public-facing does not imply that devices are public-facing
  - **Flipping roles:** cars serve user requests but act in HTTP client role, not HTTP server role
    - Infrastructure is identified by URLs and authenticated through SSL/TLS server authentication – the traditional approach in the Web
    - Car is identified by IMSI and authenticated by knowledge of random values (pushed with instruction message to IMSI) – resembling current approaches in e.g. electronic banking (buzzwords: mobile OTP/TAN)
- But it does **not** provide an overall solution for authentication in the Web-of-Things
  - The required **device connectivity** will not always be supplied in form of virtual private networks or by mobile network operators
  - Embedding mobile network endpoints incl. SIM cards and managing their contracts is feasible for things of a certain **object size** (say >1m^3) and **value** (say >10.000$)

How Will It Look Like?

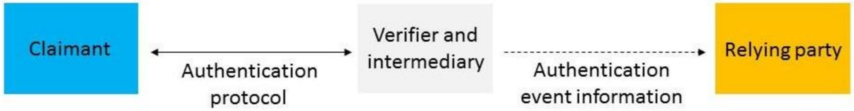
Direct:



Examples: WLAN authentication (shared secret key)
Occurrence: ubiquitous (network access), rare (Web applications)

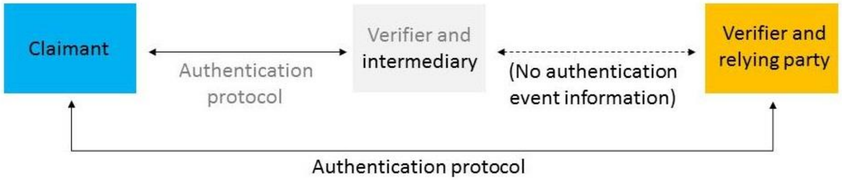
Reverse proxies externalizing initial user authn to login applications

Inline third-party, trusted:



Examples: HTTP Basic
Occurrence: ubiquitous (multi-tiered Web applications, e.g. Java EE)

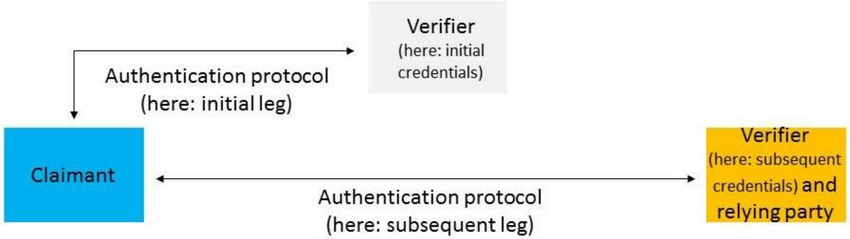
Inline third-party, untrusted:



Claimant
Authentication protocol
Verifier and intermediary
(No authentication event information)
Verifier and relying party
Authentication protocol

Examples: OAuth (authz code)
Occurrence: increasing (composite applications, mash-ups)

Online third-party, trusted:



Verifier (here: initial credentials)
Authentication protocol (here: initial leg)
Claimant
Authentication protocol (here: subsequent leg)
Verifier (here: subsequent credentials) and relying party

Examples: Kerberos, SAML, OID, OIDC
Occurrence: ubiquitous (Windows domains, Web SSO systems, social login)

OAuth authz endpoints externalizing initial user authn to login applications

So, Why Am I Here?

- ***Mantra***:
  - *Security is a key concern of distributed IT-systems*
  - *Authentication is a key discipline in IT-security*
  - *There are prerequisites for authentication as well as aftermaths*
    - *Prerequisites: management of entity identities and credentials*
    - *Aftermaths: SSO (preserving authentication), authorization and personalization (consuming it)*
- In the past 30 years the main focus was on authenticating **human users** to Internet and Intranet applications esp. **Web applications** (and vice versa):
  - A set of mechanisms, solutions and practices was established which enable the Web that we know
    - Modulo some tweaks e.g.
      - ➢ What's beyond static passwords?
      - ➢ Do people really comprehend SSL/TLS server authentication?
    - Some of that innovation is recent e.g. context-based, adaptive user authentication or OAuth
- This helps but also leaves a bulk of challenges for the Web-of-Things–we'll have an **exciting decade**:
  - Authenticating users to devices (and vice versa): accommodate intermediaries, support non-HTTP protocols, establish user-managed authorization…
  - Authenticating devices to applications as well as other devices: define and manage device identity and credentials, protect their bindings to devices, implement authentication protocols and infrastructure, establish user-managed authorization...

Author

Dr. Oliver Pfaff

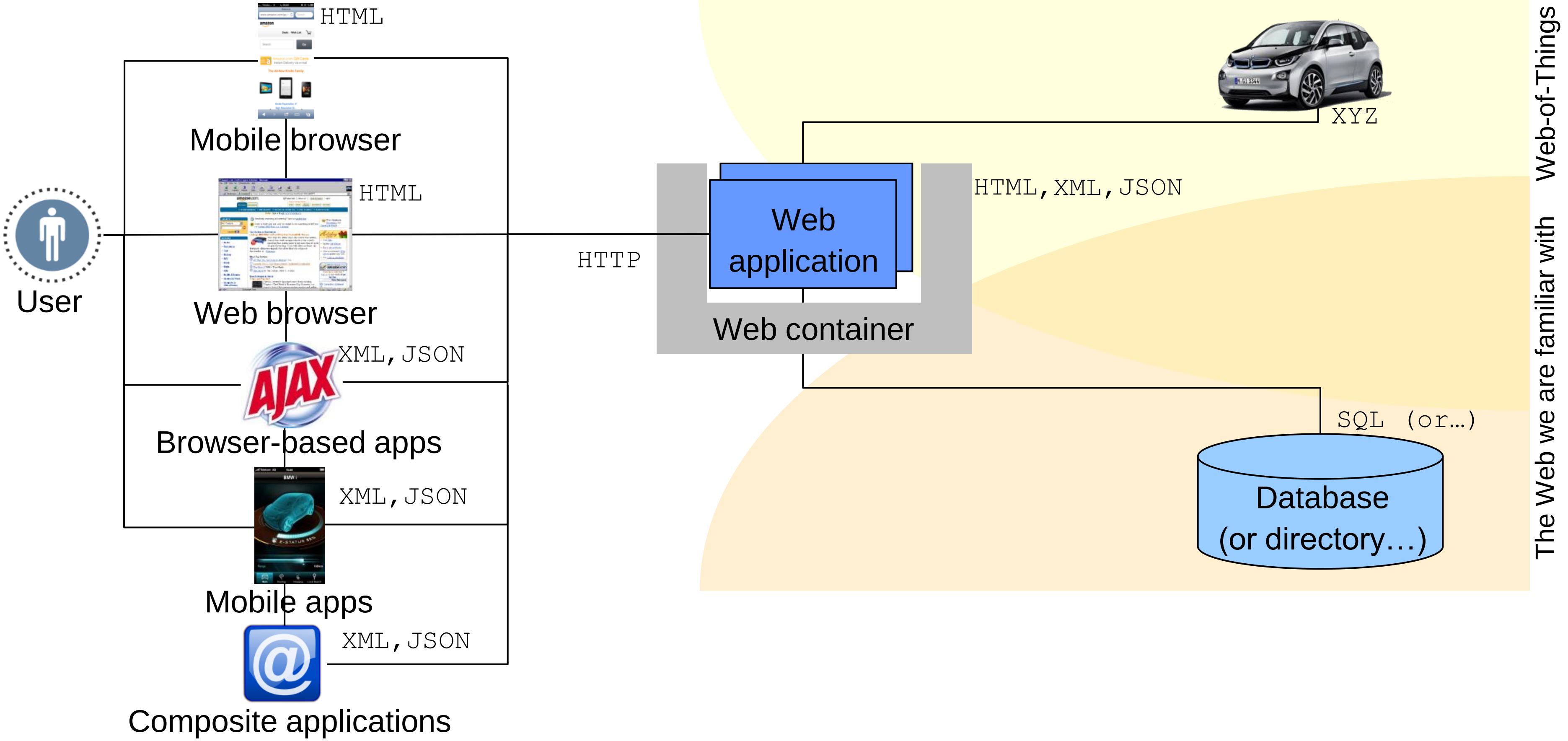
Siemens AG, CT RTC ITS

oliver.pfaff@siemens.com

Abbreviations

Authn	Authentication
Authz	Authorization
CAN	Controller Area Network
CRM	Customer Relationship Management
HTTP	HyperText Transfer Protocol
IAM	Identity and Access Management
Id	Identifier
IMSI	International Mobile Subscriber Identity
IoT	Internet-of-Things
IT	Information Technology
Java EE	Java Enterprise Edition
OAuth	Open Authorization
OID	OpenID
OIDC	OpenID Connect
OTP	One-Time Password
SAML	Security Assertion Markup Language
SIM	Subscriber Identity Module
SSL	Secure Sockets Layer
SSO	Single-Sign-On
TAN	TransAction Number
TLS	Transport Layer Security
URL	Uniform Resource Locator
VIN	Vehicle Identification Number
WLAN	Wireless Local Area Network
WoT	Web-of-Things

How Does the Web Evolve?



1995 **Database-backed applications**, desktop browsers, read-only

2000 Read/write aka **Web 2.0**, AJAX clients

2005 **Mobile** browsers/apps, **Composite** applications

2010 **Things-backed applications**