SIEMENS

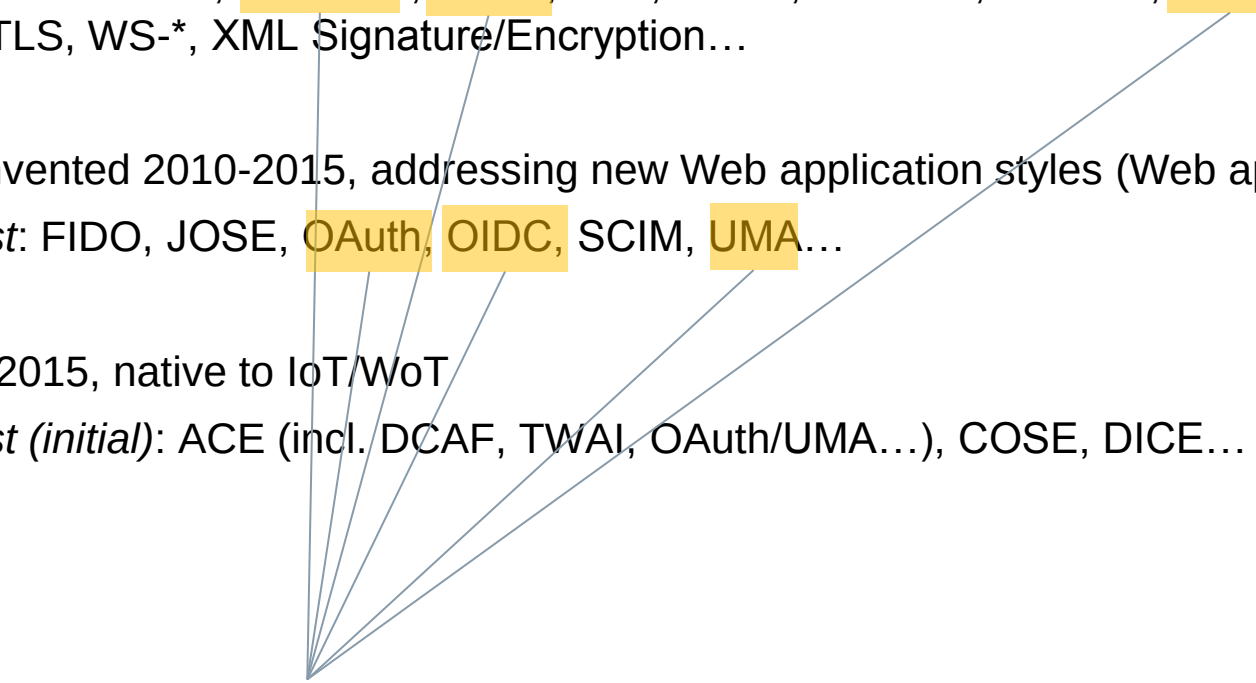
Siemens Corporate Technology | July 2015

Joint IRTF T2T RG / W3C WoT IG Meeting 18-19 July 2015, Prague

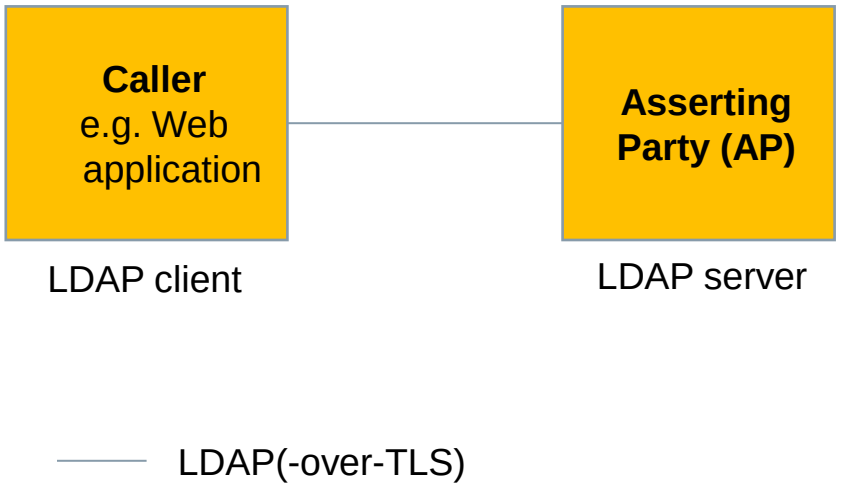
Existing Infrastructure vs. New Challenges

Our Security&Privacy Menu

- **Classic**:
  - *Synopsis*: invented <2010, native to enterprise/office-IT resp. traditional Web
  - *Shopping list*: Diameter, Kerberos, LDAP, P3P, PKCS, RADIUS, S/MIME, SAML, SSL/TLS/DTLS, WS-*, XML Signature/Encryption…
- **New**:
  - *Synopsis*: invented 2010-2015, addressing new Web application styles (Web apps/APIs)
  - *Shopping list*: FIDO, JOSE, OAuth, OIDC, SCIM, UMA…
- **Future**:
  - *Synopsis*: >2015, native to IoT/WoT
  - *Shopping list (initial)*: ACE (incl. DCAF, TWAI, OAuth/UMA…), COSE, DICE…

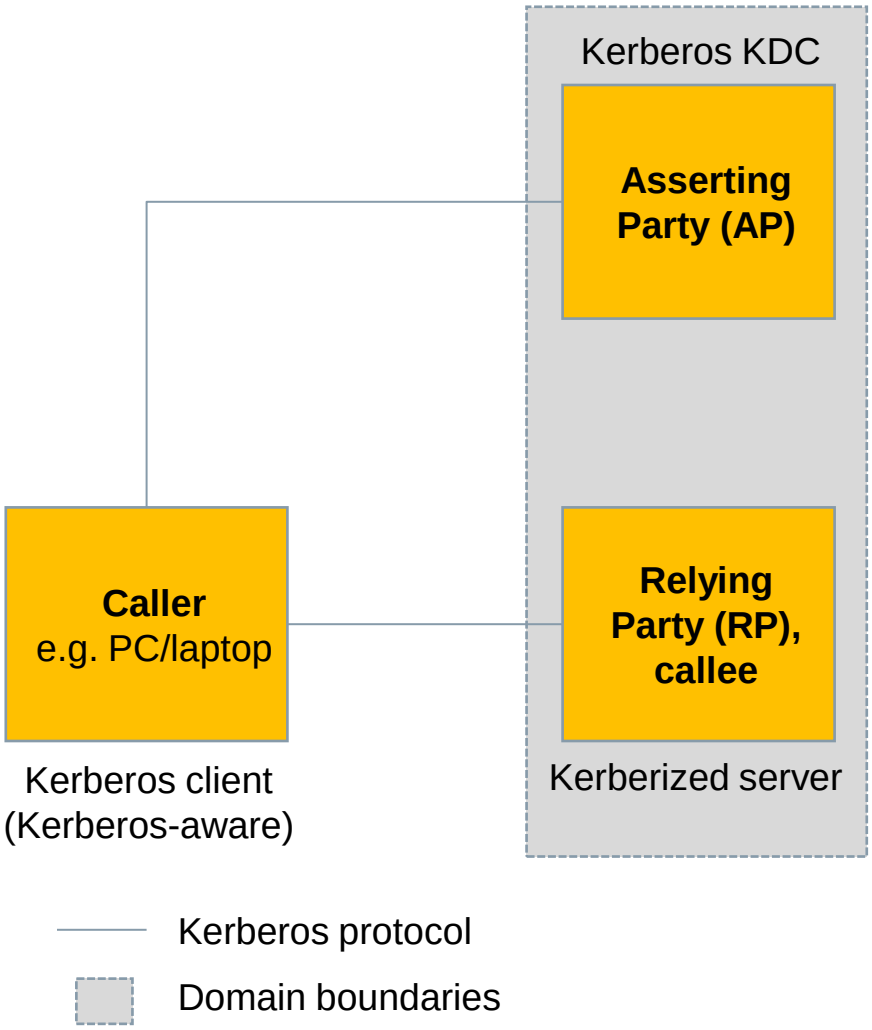


LDAP 3.0



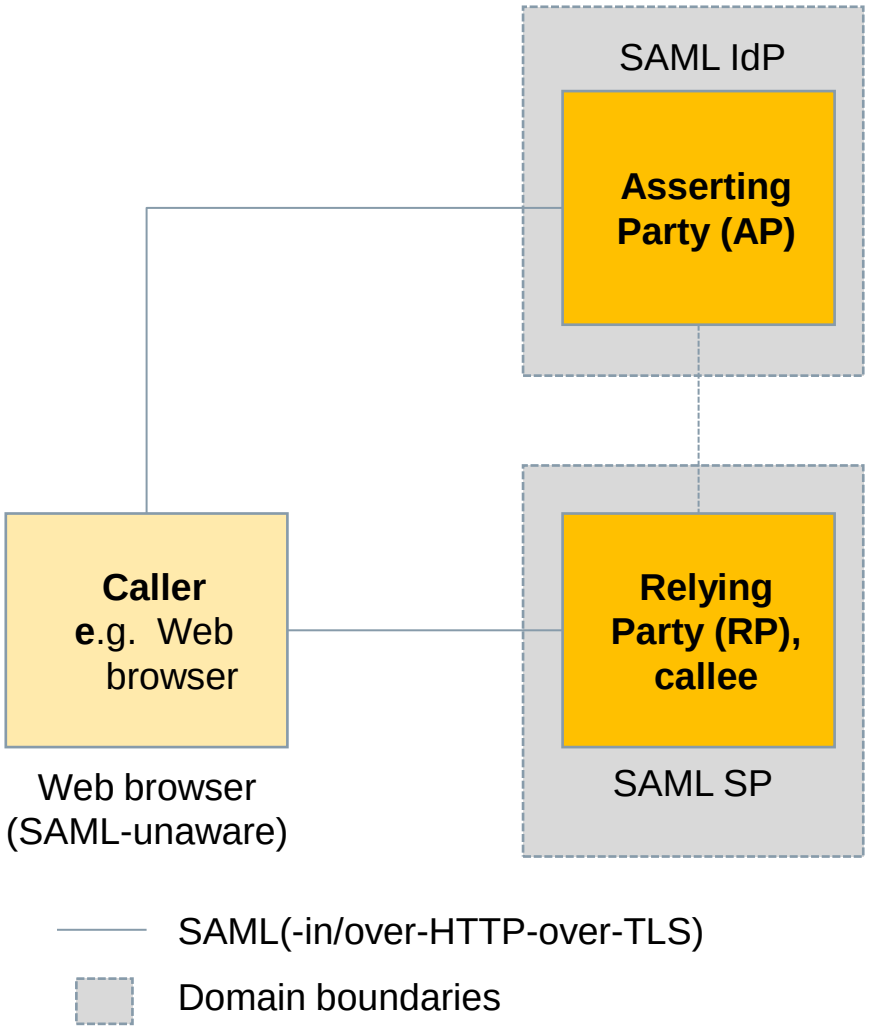
- **Focus**:
  - **User data**: store for identifiers, credentials attributes, affiliations, login metadata
  - **User authentication**: internalized (LDAP Bind)
- **Features**:
  - Initial authentication with username/password
  - Password polices (LPPE)
  - Persisted, hierarchically-structured data store
- **Limitations**:
  - Initial authentication schemes other than username/password
  - No security token
  - No SSO or persisted login UX
  - AP resp. caller components upon constrained devices
- **Significance**: ubiquitous technology for user data stores (enterprise/office-IT, Web)

Kerberos 5.0



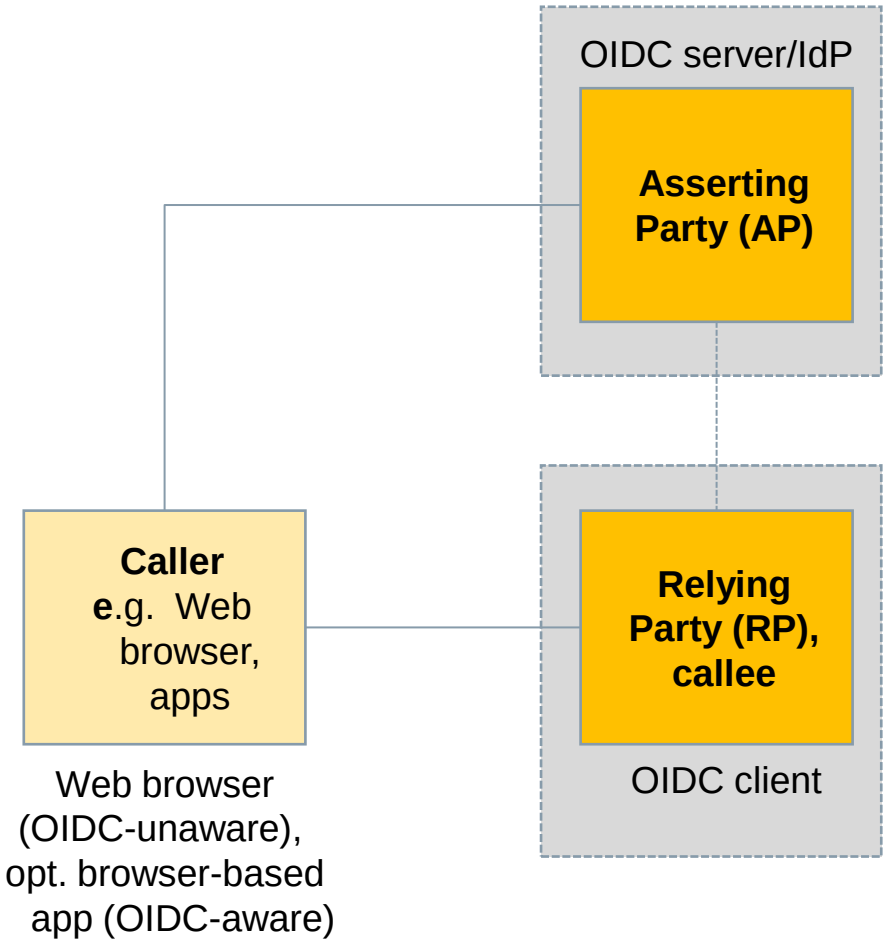
- **Focus**:
  - **User authentication**: internalized (@AP)
  - **SSO-UX**: same/cross-domain
- **Features**:
  - Password or PKI-based user authentication
  - PoP security tokens (ASN.1)
  - SSO-UX in the same organization
  - Some persisted login UX (by means of TGTs)
  - Extensions (S4U)
- **Limitations**:
  - Initial authentication schemes other than password or PKI-based
  - No rich metadata about initial authentication
  - No cross-organization SSO-UX
  - AP/RP resp. caller/callee components upon constrained devices
- **Significance**: ubiquitous use in enterprise-IT

SAML 2.0



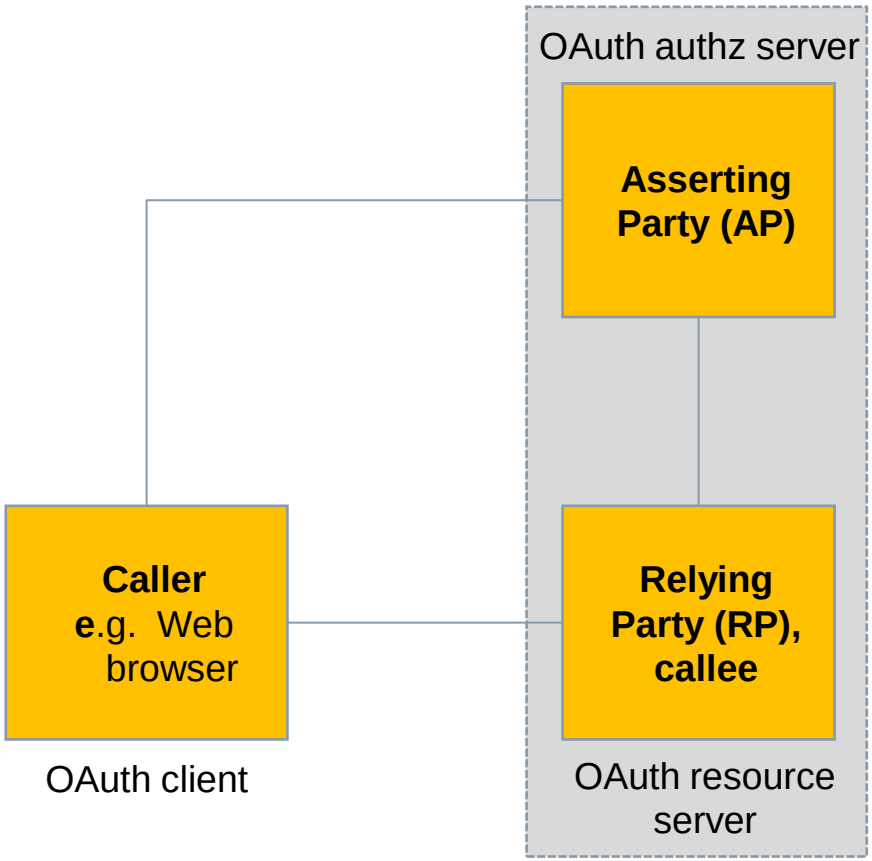
- **Focus**:
  - **User authentication**: externalized
  - **SSO-UX**: cross-organization/domain
- **Features**:
  - SSO-UX and federated identity for Web
  - Rich metadata about initial authentication
  - (Bearer) security tokens (XML): versatile contents statically issued according RP needs
- **Limitations**:
  - RP simplicity
  - Ad-hoc registration of RPs at APs (without explicit administrative action)
  - No persisted login UX
  - Non-HTTP
  - AP/RP resp. callee components upon constrained devices
- **Significance**: moderate use in enterprise/higher education IT

OIDC 1.0 (an OAuth 2.0 Descendant)



- **Focus**:
  - **User authentication**: externalized
  - **SSO-UX**: cross-organization/domain
- **Features**:
  - SSO-UX and federated identity for Web
  - Rich metadata about initial authentication
  - Bearer security tokens (JSON): versatile contents dynamically issued according RP needs
  - RP simplicity
  - Ad-hoc registration of RPs at APs (without explicit administrative action)
- **Limitations**:
  - No login UX across apps
  - Non-HTTP
  - AP/RP resp. callee components upon constrained devices
- **Significance**: vast coverage of the 7''' human users on Earth: Amazon, (Facebook), Google…

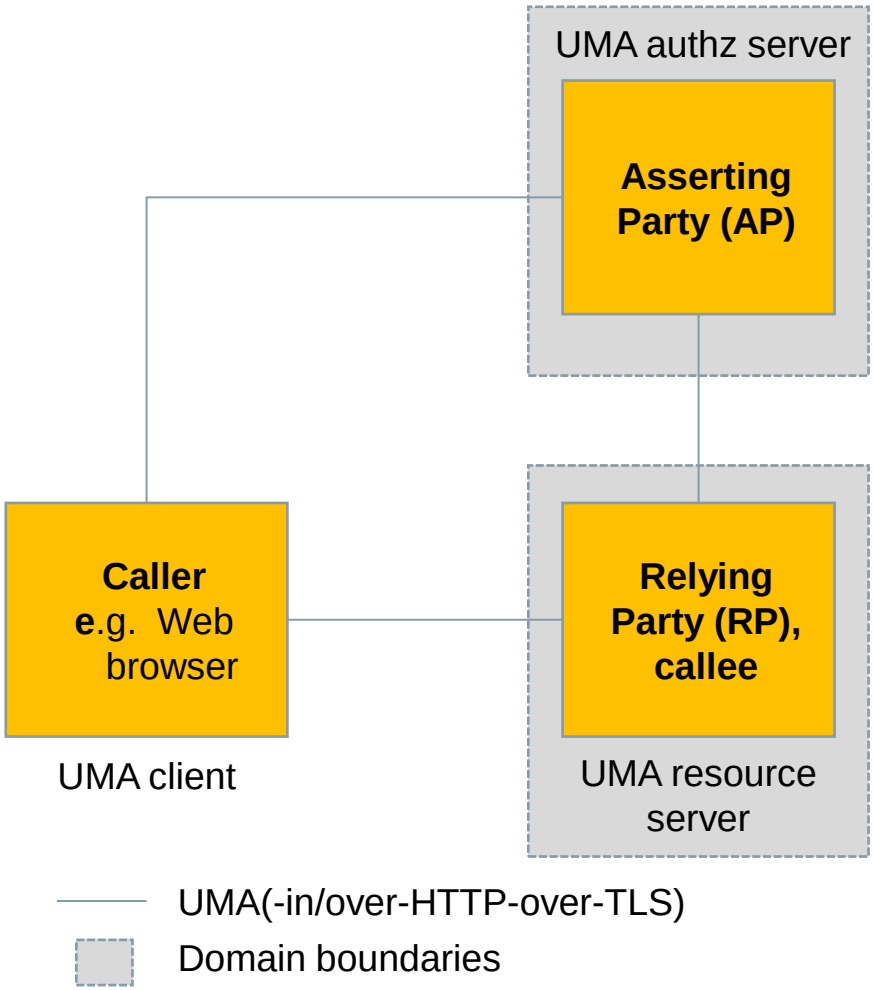
OAuth 2.0



Caveat: OAuth is a zoo, this slide considers the native OAuth use case aka authz code grant

- **Focus**:
  - **Authorization**: owner-to-self
  - **User authentication**: persisted login UX
- **Features**:
  - Authorization for Web resources owned by individual end users (for self)
  - RP simplicity
  - Ad-hoc registration of RPs at APs (without explicit administrative action)
- **Limitations**:
  - Owner-to-any authorization
  - Non-HTTP
  - AP/(RP) resp. caller/(callee) components upon constrained devices
- **Significance**: ubiquitous means to protect Web APIs and to implement persisted login UX in mobile apps

UMA 1.0 (an OAuth 2.0 Descendant)



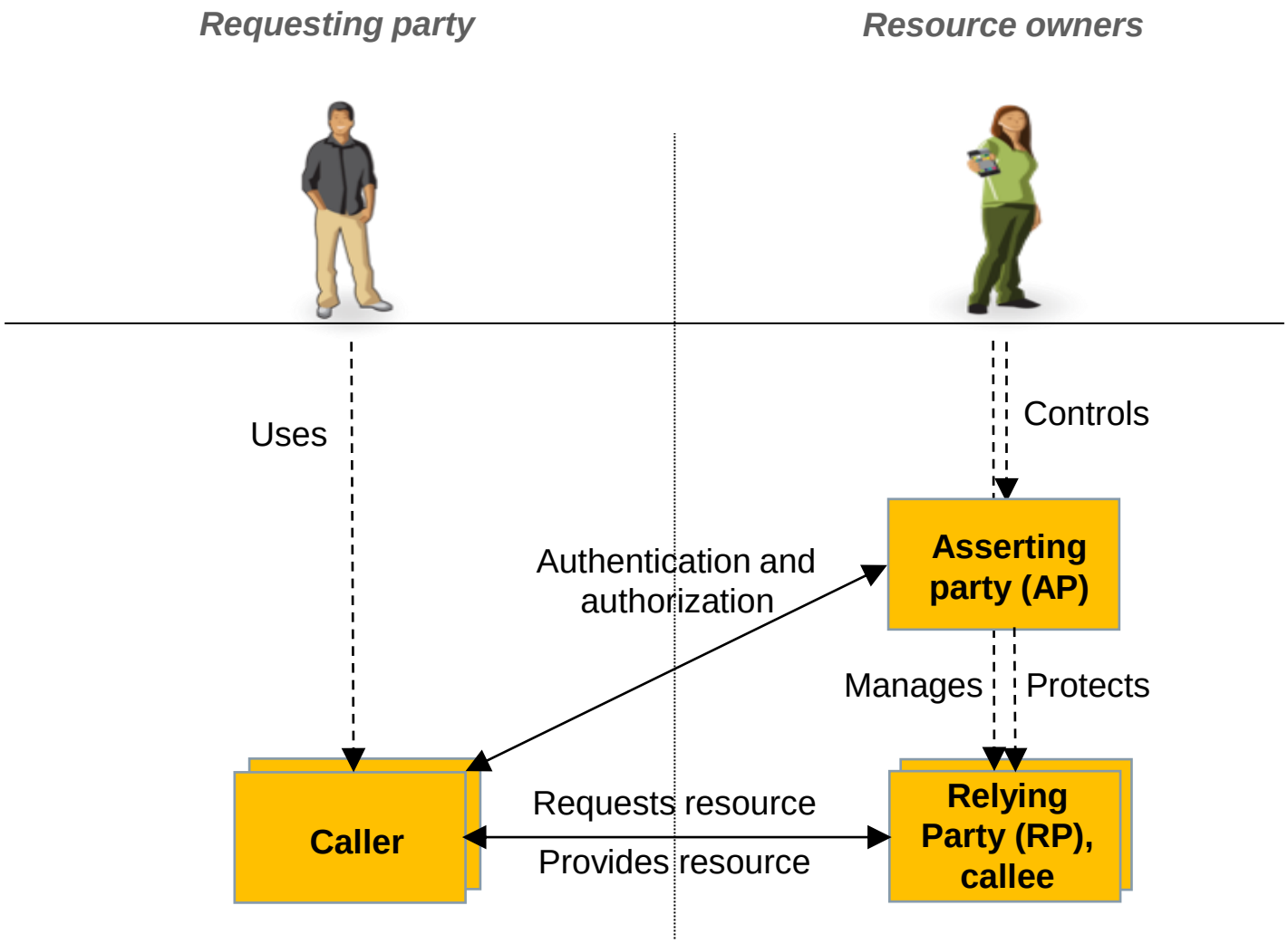
- **Focus**:
  - **Authorization**: owner-to-any
- **Features**:
  - Authorization for Web resources owned by individual end users (for others)
- **Limitations**:
  - Non-HTTP
  - AP/RP resp. callee/caller components upon constrained devices
- **Significance**: sporadically used means to protect Web applications

Pattern of Common AAA Technologies: Kerberos, OAuth, UMA

SIEMENS

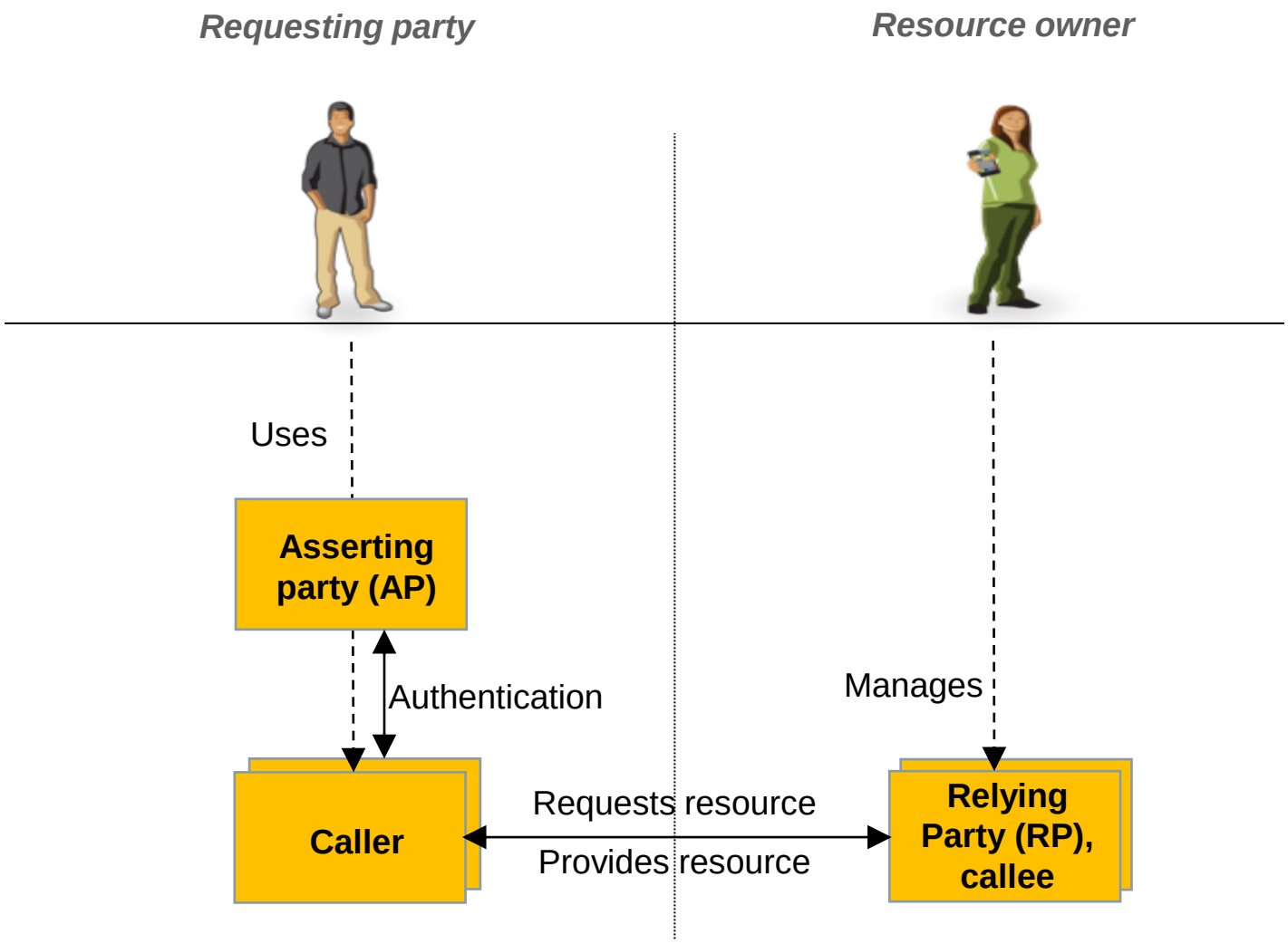
Principals
(individuals, companies)

Components



Pattern of Common AAA Technologies: SAML, OIDC

SIEMENS



Conclusions (1)

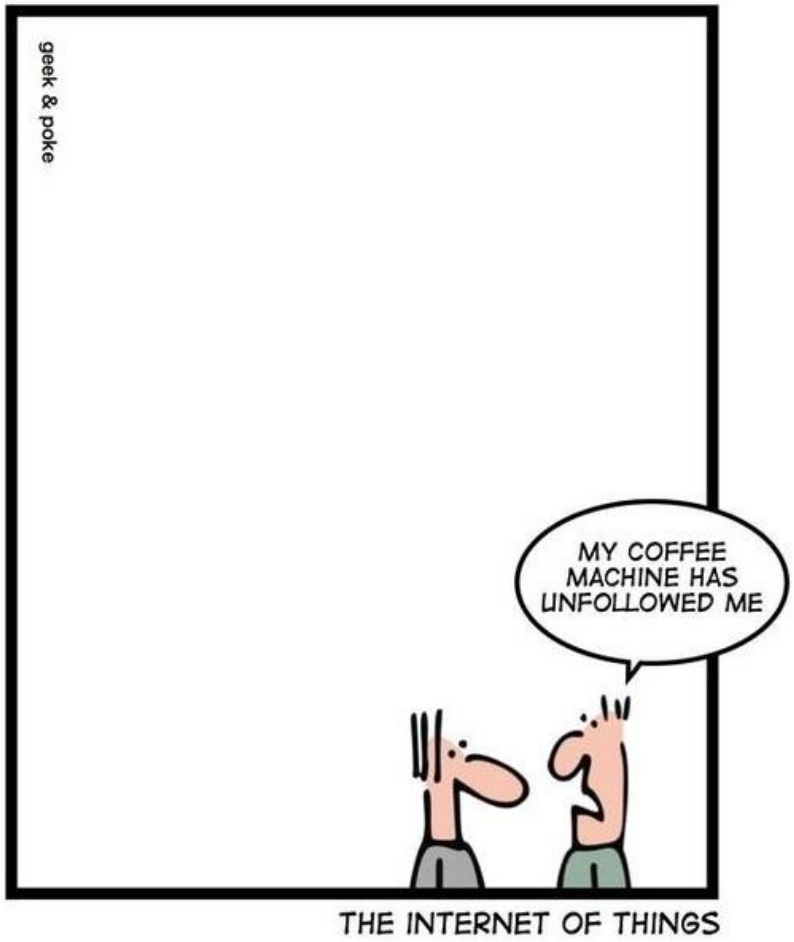
- *Entity infrastructure*:
  - **Human users - addressed**
    - Employees: covered (enterprise user repositories and authentication systems), re-use/extend
    - Consumers: depends from where one starts
  - **Clients/services – addressed**
    - Office/enterprise-IT: covered (Windows domain infrastructure)
    - Web: server authentication (SSL/TLS), OAuth-based client registration/authentication
  - **Things/devices – not addressed**
    - Investment goods: not covered
    - Consumer goods: not covered

Conclusions (2)

- *Technology stacks*:
  - **Human users – re-use, integrate**
  - **Clients/services – re-use, integrate**
  - **Things/devices – invent**
    - Classic and new technologies focus on authorization, authentication and identity for human users, lack corresponding support of (unattended) **devices/things**
    - Lack support for AP/RP resp. caller/callee **components upon constrained devices** (RFC 7228 device classes 0/1/2)
    - Lack support of **change-of-ownership use case**
- *More information*: see W3C WoT IG Wiki page **Landscape of Security&Privacy Means**

Summary ;-)

This use case is not really thought of in contemporary IT-security:



Abbreviations

AAA	Authentication, Authorization, Accounting
ACE	Authentication and Autorisation for Constrained Environment
AP	Asserting Party
ASN.1	Abstract Syntax Notation 1
Authn	Authentication
Authz	Authorization
CBOR	Concise Binary Object Representation
CoAP	Constrained Application Protocol
COSE	CBOR Object Signing and Encryption
DICE	DTLS In Constrained Environments
DTLS	Datagram TLS
FIDO	Fast Identity Online
HTTP	HyperText Transfer Protocol
I4.0	Industrie 4.0 (German term)
IdP	Identity Provider
IIC	Industrial Internet Consortium
IoT	Internet-of-Things
JOSE	Javascript Object Signing and Encryption
JSON	JavaScript Object Notation
LDAP	Lightweight Directory Access Protocol
LPPE	LDAP Password Policy Extensions
MIME	Multipurpose Internet Mail Extensions
OAuth	Open Authorization
OIDC	OpenID Connect
P3P	Platform for Privacy Preferences
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PoP	Proof-of-Possession
RADIUS	Remote Authentication Dial-In User Service
RP	Relying Party
S4U	Service for User
S/MIME	Secure MIME
SAML	Security Assertion Markup Language
SCIM	System for Cross-Domain Identity Management
SSL	Secure Sockets Layer
TGT	Ticket Granting Ticket
TLS	Transport Layer Security
TWAI	Two-Way Authentication for IoT
UMA	User-Managed Access
UX	User eXperience
WoT	Web-of-Things
WS	Web Services
XML	eXtensible Markup Language

Author

Oliver Pfaff, Siemens AG, CT RTC ITS