protégé

8th Intl. Protégé Conference - July 18-21, 2005 - Madrid, Spain

An Ontology for Generic Wireless Authentication Data

Asma Alazeib, Hamburg University of Technology, Germany
Andreas Diehl, University of Plymouth, UK
In co-operation with Alcatel SEL AG, Germany

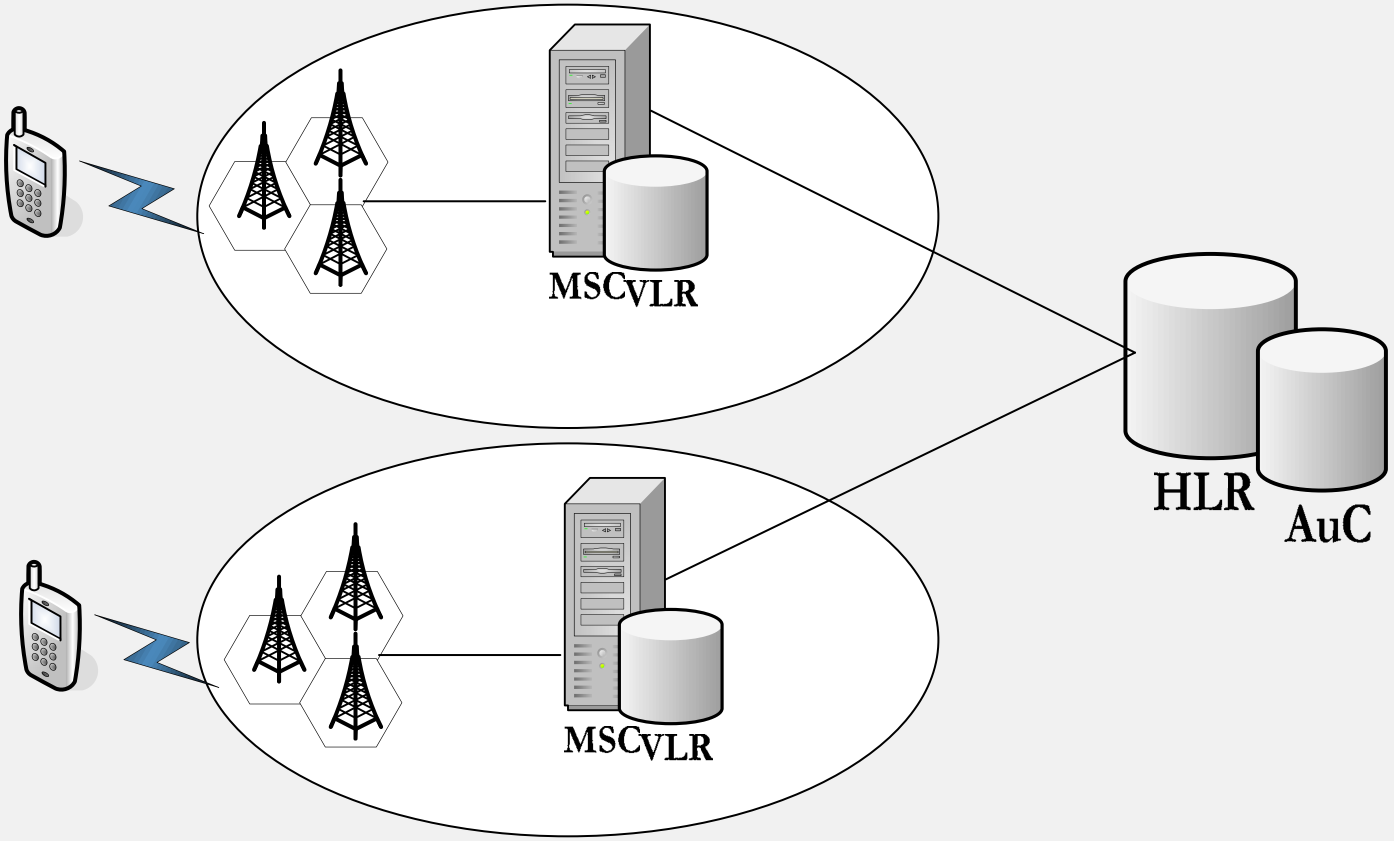
July 20th, 2005

Outline

- Introduction to the GSM Network
- Restructuring of the Wireless Telecommunication Networks
- GSM, UMTS, WLAN Authentication
- Overview of our Ontology
- Future data integration
- Conclusions

The GSM Network

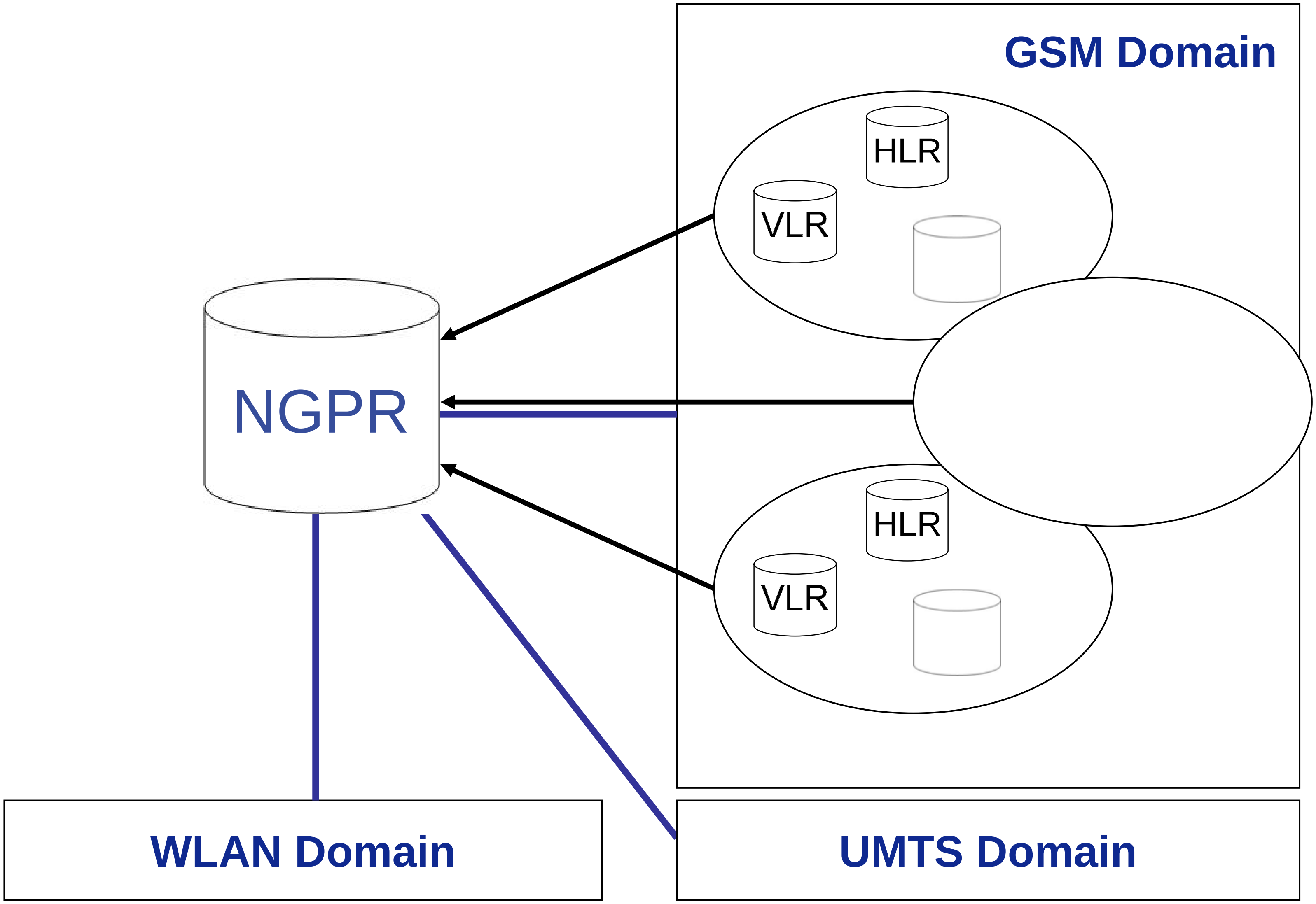
- Each area owns the main GSM subscriber database (HLR)
- Subscriber data is distributed all over a network (country)
- Services/applications have to be deployed for each area



Problems of Wireless Telecom. Providers

- Distributed subscriber profiles
- Distributed applications and data
- No complete subscriber profile
- Various local applications (e.g. billing, CRM) for one user
- Closed mobile networks (difficult integration of Third Party applications)
- Vendor dependent network nodes
- Long installation/deployment time for new services
- → Complex and diverse networks

Restructuring Telecom. Networks I



Advantages of a restructured network

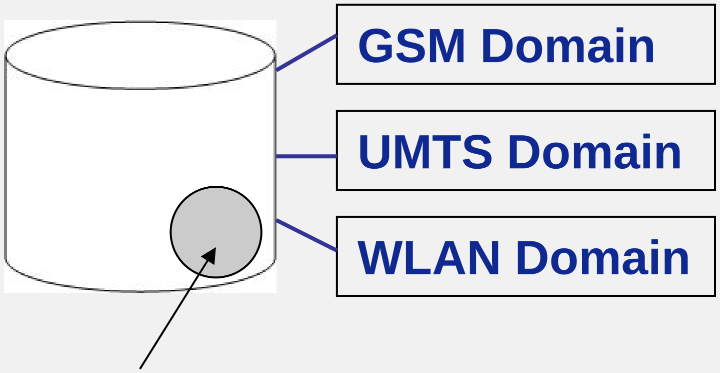
- Integration of all access networks (domains) of the operator
- Re-usage of data and services for different access networks
- Access for the complete subscriber profile
- Reduced network complexity
- Simple support of seamless services
- Faster service access and deployment
- Reduced maintenance costs

Protégé OWL for Data Modelling

- No 3GPP data model definition
- Semantic Description of data
  - Network and area/location dedication (e.g. network nodes, algorithms)
  - XML-based standard for semantic applications
  - Common user data (meta-data)
  - Separation of domain and operational knowledge (e.g. extension of GSM services)
  - Analysis and re-use of domain knowledge
  - Formal description of service features and the overall concept
- Better expressiveness compared to concrete data models (e.g. relational, UML/OO, XML-Schema)
- Implementation independent description of data
- Logical description and reasoning of data

Our Concentration

- Different types of data stored in the NGPR
- Service and application specific data
- Our concentration: Authentication specific data



GSM Domain

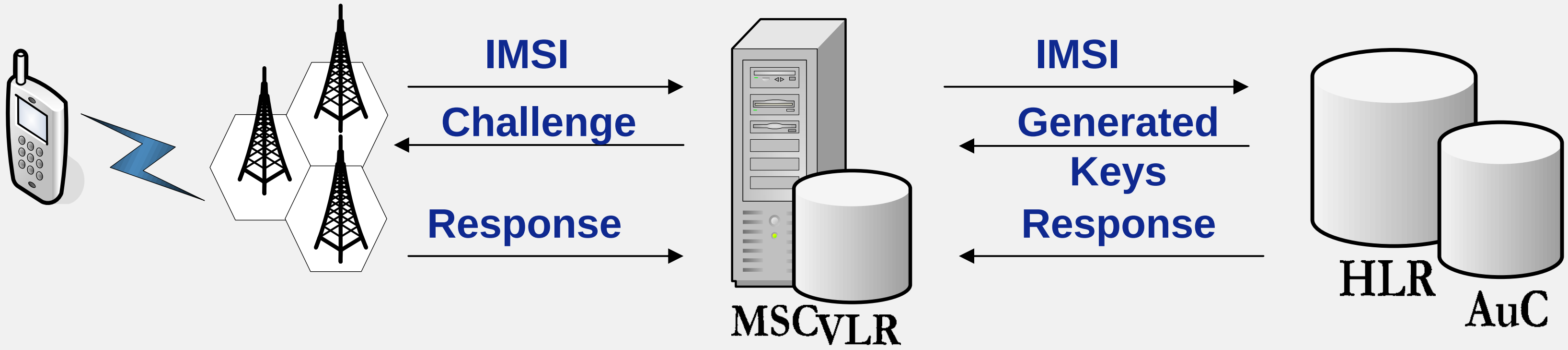
UMTS Domain

WLAN Domain

Authentication Specific Data

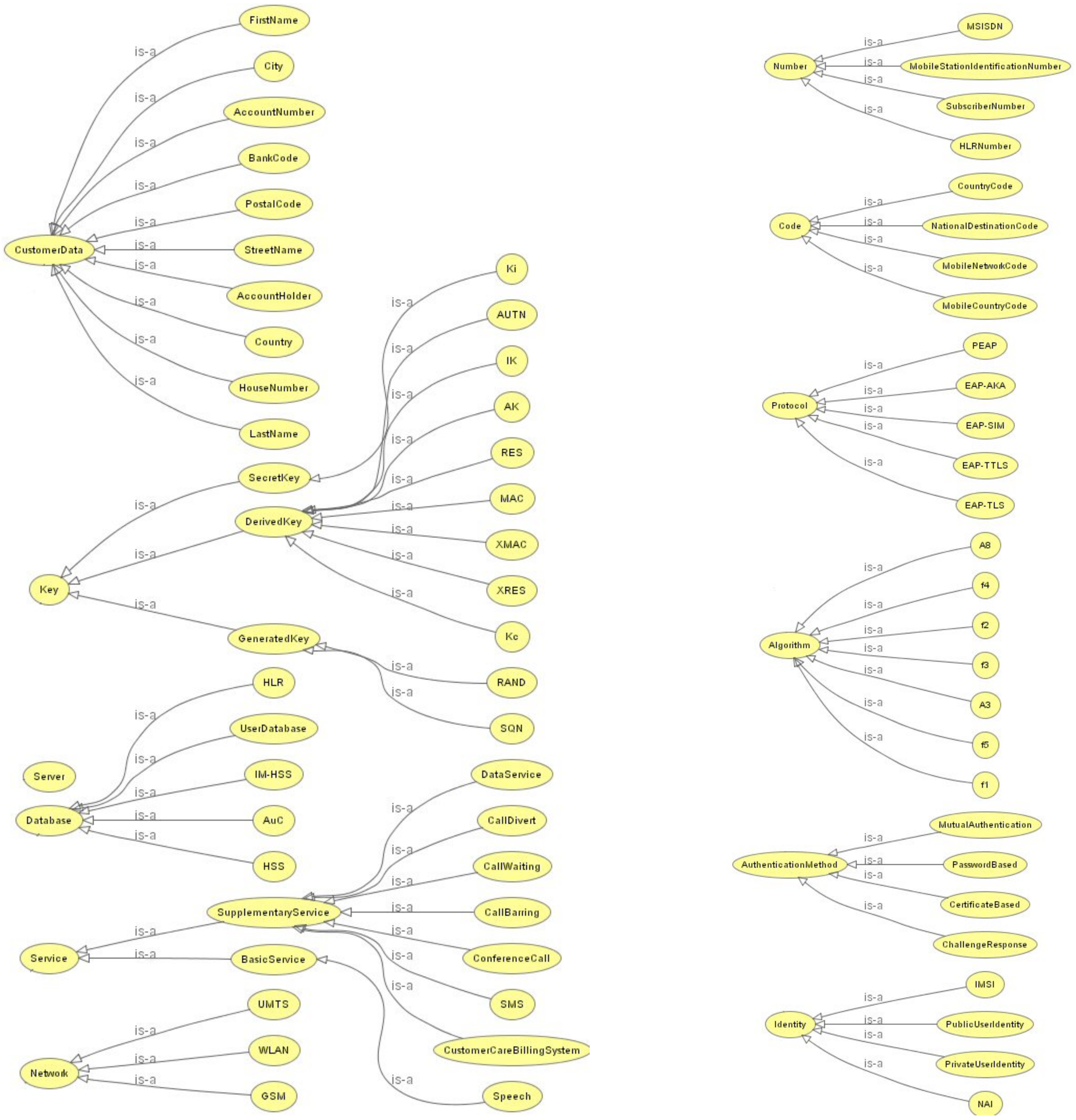
GSM Authentication

- Challenge/Response Authentication
- IMSI as proof of identity
- Challenge to calculate response
- Network and user side response
- Same response = successful authentication

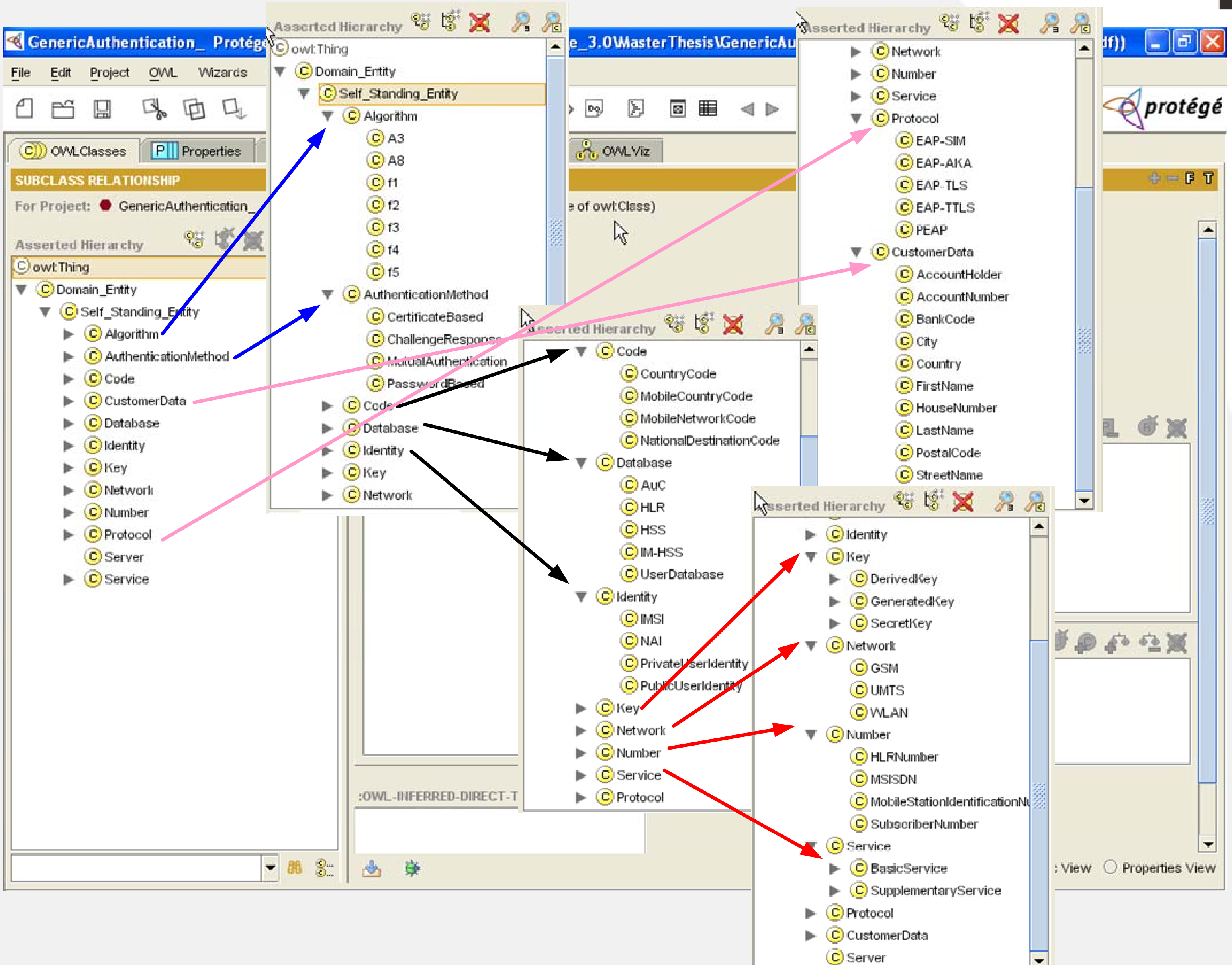


Authentication in Other Networks

- GSM: Only user is authenticated
- UMTS:
  - Similar to GSM Authentication, but
    - Different keys and algorithms used
    - Mutual Authentication
- WLAN: Authentication methods not standardized.
  - Password and Certificate based methods


CustomerData
FirstName
City
AccountNumber
BankCode
PostalCode
StreetName
AccountHolder
Country
HouseNumber
LastName
Key
SecretKey
DerivedKey
GeneratedKey
Ki
AUTN
IK
AK
RES
MAC
XMAC
XRES
Kc
RAND
SQN
Server
Database
HLR
UserDatabase
IM-HSS
AuC
HSS
Service
SupplementaryService
BasicService
DataService
CallDivert
CallWaiting
CallBarring
ConferenceCall
SMS
CustomerCareBillingSystem
Speech
Network
UMTS
WLAN
GSM
Number
MSISDN
MobileStationIdentificationNumber
SubscriberNumber
HLRNumber
Code
CountryCode
NationalDestinationCode
MobileNetworkCode
MobileCountryCode
Protocol
PEAP
EAP-AKA
EAP-SIM
EAP-TTLS
EAP-TLS
Algorithm
A8
f4
f2
f3
A3
f5
f1
AuthenticationMethod
MutualAuthentication
PasswordBased
CertificateBased
ChallengeResponse
Identity
IMSI
PublicUserIdentity
PrivateUserIdentity
NAI
is-a

Classes and Subclasses



Asserted Hierarchy

- owl:Thing
  - Domain_Entity
    - Self_Standing_Entity
      - Algorithm
      - AuthenticationMethod
      - Code
      - CustomerData
      - Database
      - Identity
      - Key
      - Network
      - Number
      - Protocol
      - Server
      - Service

Asserted Hierarchy

- owl:Thing
  - Domain_Entity
    - Self_Standing_Entity
      - Algorithm
        - A3
        - A8
        - f1
        - f2
        - f3
        - f4
        - f5
      - AuthenticationMethod
        - CertificateBased
        - ChallengeResponse
        - MutualAuthentication
        - PasswordBased
      - Code
      - Database
      - Identity
      - Key
      - Network

Asserted Hierarchy

- Code
  - CountryCode
  - MobileCountryCode
  - MobileNetworkCode
  - NationalDestinationCode
- Database
  - AuC
  - HLR
  - HSS
  - IM-HSS
  - UserDatabase
- Identity
  - IMSI
  - NAI
  - PrivateUserIdentity
  - PublicUserIdentity
- Key
- Network
- Number
- Service
- Protocol

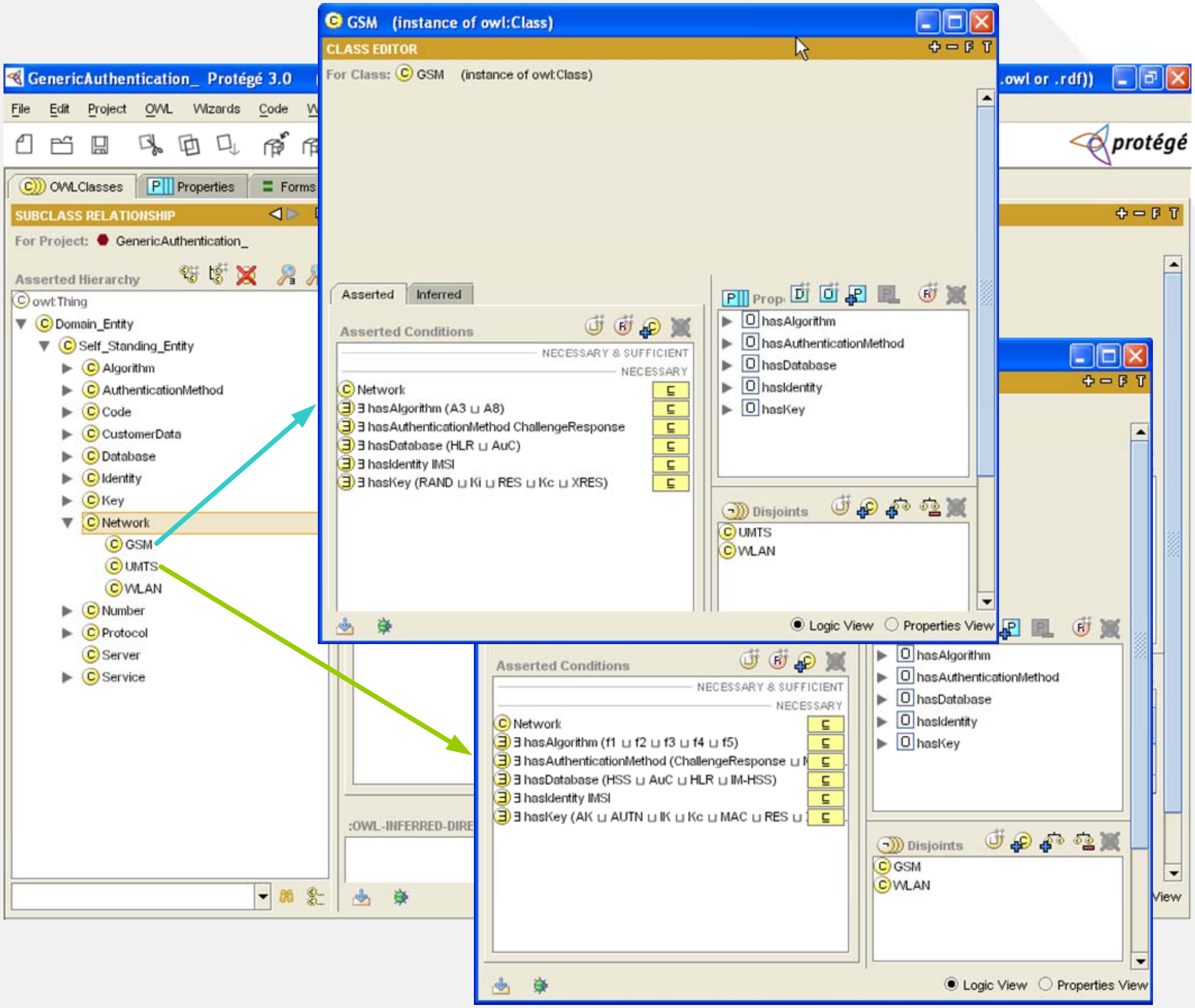
Asserted Hierarchy

- Network
- Number
- Service
- Protocol
  - EAP-SIM
  - EAP-AKA
  - EAP-TLS
  - EAP-TTLS
  - PEAP
- CustomerData
  - AccountHolder
  - AccountNumber
  - BankCode
  - City
  - Country
  - FirstName
  - HouseNumber
  - LastName
  - PostalCode
  - StreetName

Asserted Hierarchy

- Identity
- Key
  - DerivedKey
  - GeneratedKey
  - SecretKey
- Network
  - GSM
  - UMTS
  - WLAN
- Number
  - HLRNumber
  - MSISDN
  - MobileStationIdentificationN
  - SubscriberNumber
- Service
  - BasicService
  - SupplementaryService
- Protocol
- CustomerData
- Server

GSM and UMTS Classes


GenericAuthentication_ Protégé 3.0
File Edit Project OWL Wizards Code W
OWLClasses Properties Forms
.owl or .rdf))
protégé
SUBCLASS RELATIONSHIP
CLASS EDITOR
Asserted Inferred
Prop
Logic View Properties View
:OWL-INFERRED-DIRE
View

For Project: GenericAuthentication_

Asserted Hierarchy

- owl:Thing
- Domain_Entity
  - Self_Standing_Entity
    - Algorithm
    - AuthenticationMethod
    - Code
    - CustomerData
    - Database
    - Identity
    - Key
    - Network
      - GSM
      - UMTS
      - WLAN
    - Number
    - Protocol
    - Server
    - Service

GSM (instance of owl:Class)

For Class: GSM (instance of owl:Class)

Asserted Conditions

NECESSARY & SUFFICIENT

NECESSARY

Network ⊑
∃ hasAlgorithm (A3 ⊔ A8) ⊑
∃ hasAuthenticationMethod ChallengeResponse ⊑
∃ hasDatabase (HLR ⊔ AuC) ⊑
∃ hasIdentity IMSI ⊑
∃ hasKey (RAND ⊔ Ki ⊔ RES ⊔ Kc ⊔ XRES) ⊑

hasAlgorithm
hasAuthenticationMethod
hasDatabase
hasIdentity
hasKey

Disjoints

UMTS
WLAN

● Logic View ○ Properties View

Asserted Conditions

NECESSARY & SUFFICIENT

NECESSARY

Network ⊑
∃ hasAlgorithm (f1 ⊔ f2 ⊔ f3 ⊔ f4 ⊔ f5) ⊑
∃ hasAuthenticationMethod (ChallengeResponse ⊔ I ⊑
∃ hasDatabase (HSS ⊔ AuC ⊔ HLR ⊔ IM-HSS) ⊑
∃ hasIdentity IMSI ⊑
∃ hasKey (AK ⊔ AUTN ⊔ IK ⊔ Kc ⊔ MAC ⊔ RES ⊔ ⊑

hasAlgorithm
hasAuthenticationMethod
hasDatabase
hasIdentity
hasKey

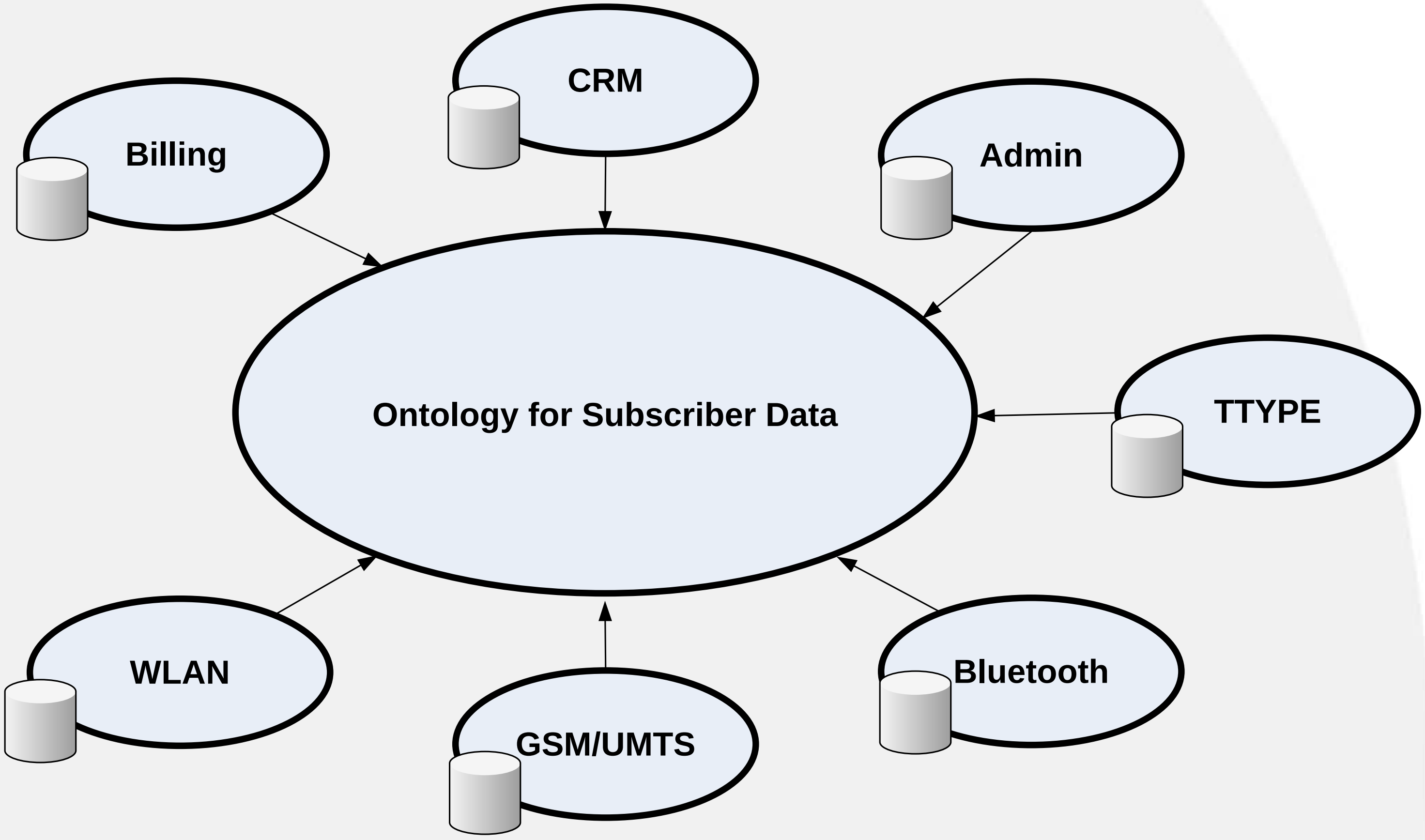
Disjoints

GSM
WLAN

● Logic View ○ Properties View

Future Work

- Addition of other domains and services



Conclusions

- Novel approach of a common authentication model for a NGPR
- Semantic model offers data translation to concrete models
- Easier view compared to relational data models
- Rich standard which provides a better vocabulary for data modelling
  - describing properties and classes
  - relations between classes
  - cardinality
  - characteristics of properties and enumerated classes

Thanks for your attention,
Questions ?