



Trusted identities for the cloud using open source technologies where Open eCard App meets SkIDentity

Tobias Wich
Dr. Detlef Hühnlein
Moritz Horsch
Johannes Schmölz



Berlin, 23.5.2012



Agenda

- Introduction
 - Identity Management
 - eCard-API-Framework
- SkIDentity
- Open eCard App
- Summary



Identities

- A „complete identity“ is the sum of all attributes of any entity
 - A „digital identity“ \subset „complete identity“
 - Or „partial identity“
-
- An Identity Management is a system responsible for the attributes of identities
 - It creates assertions for partial identities



(Site-)Local IdM Systems

- IdP (Identity Provider) and SP (Service Provider) belong to the same realm
- Not possible to use identity outside realm
- Examples
 - /etc/shadow
 - Database (SQL/LDAP)
 - ...

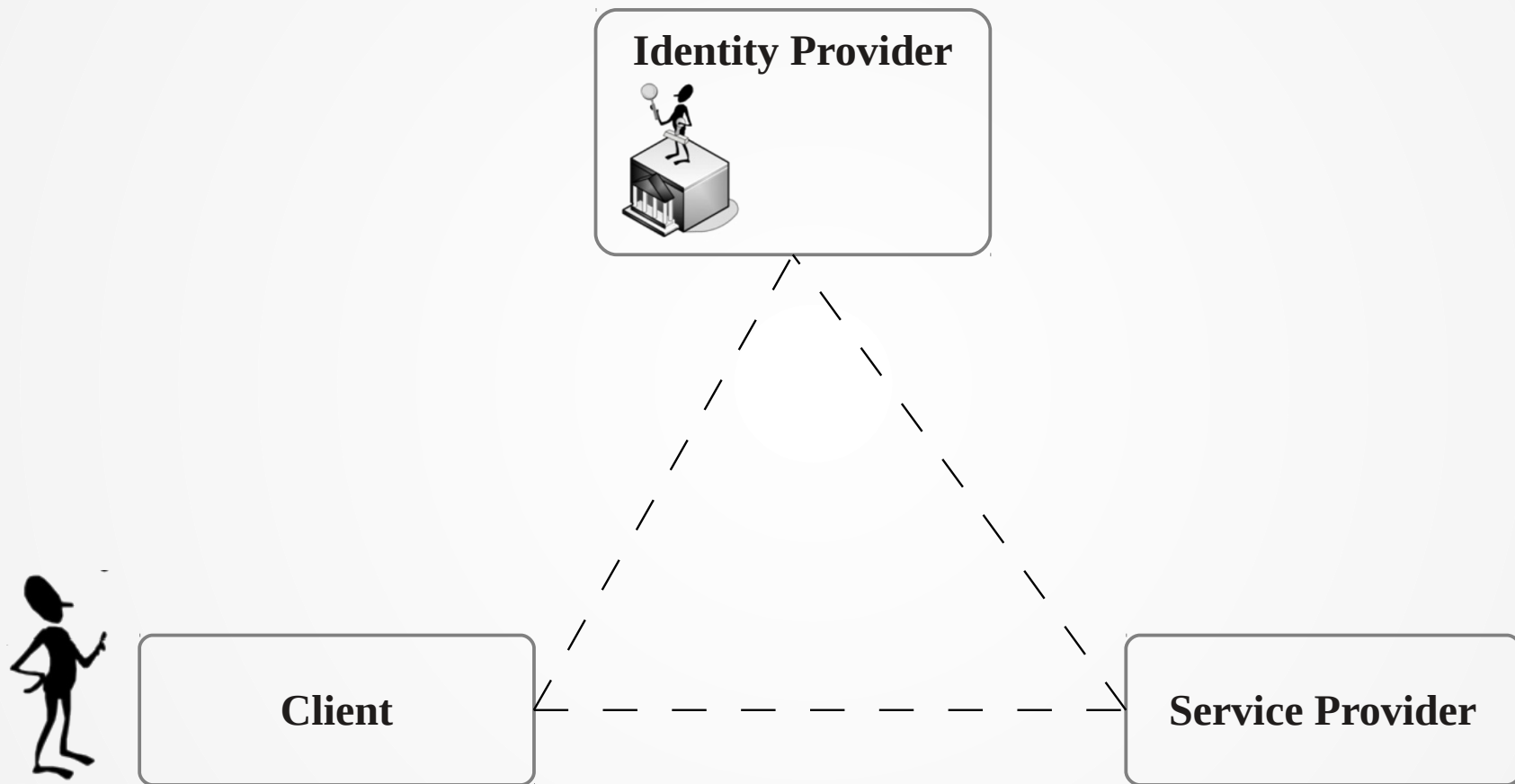


Federated IdM Systems

- IdP and SP have a trust relationship
 - IdP creates assertion of a users identity
 - SP can validate and use an assertion
- Diagram illustrating the Federated Identity Management (IdM) process:
-
- ```
graph LR; User((User)) --> IdP(IdP); IdP --> SP(SP); SP --> IdP; IdP --> User;
```
- Examples
    - Kerberos
    - SAML
    - OpenID
    - OAuth
    - ...



# Federated Architecture





# Status Quo Identity Management

- Passwords are (still) standard
- When passwords are simple, then they are
  - easy to use
  - easy to carry around (knowledge)
  - cheap
- **Therefore:** Identity theft is serious threat
  - Phishing, XSS, Sony, ...
  - In fact even worse with SSO



# Authentication Tokens

## to the rescue

- One-Time-Password (OTP) Token
  - Yubikey, Smartphone, ...
- Biometry
  - can be strong, but must not be
- X509 is the poor mans smart-card
  - Can be seen as hybrid  
(Possession of knowledge/data)
  - But fights XSS, phishing (not all) and Sony
- smart-card + PIN (+ Certificates)
  - Cards vary greatly with regard to security





# So why is nobody using it?

- Hardware-Tokens often use different Protocols
- Few client applications are ready for use with Smart-Card X
- Locked out when token is lost/defect
- Hardware has a price
- High security too



# Agenda

- Introduction
  - Identity Management
  - eCard-API-Framework
- SkIDentity
- Open eCard App
- Summary



# eCard-API-Framework

„The objective of the eCard-API-Framework is the provision of a simple and homogeneous interface to enable standardised use of the various smart cards (eCards) for different applications.“

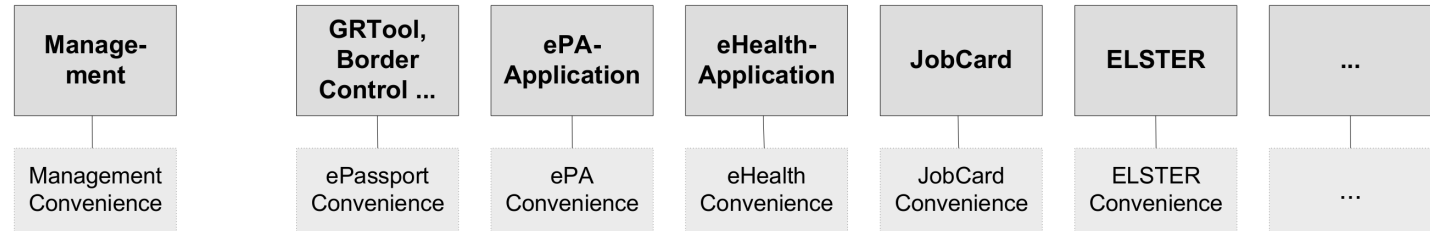
In other Words:

Network transparent abstractions of smart-cards with XML and SOAP.

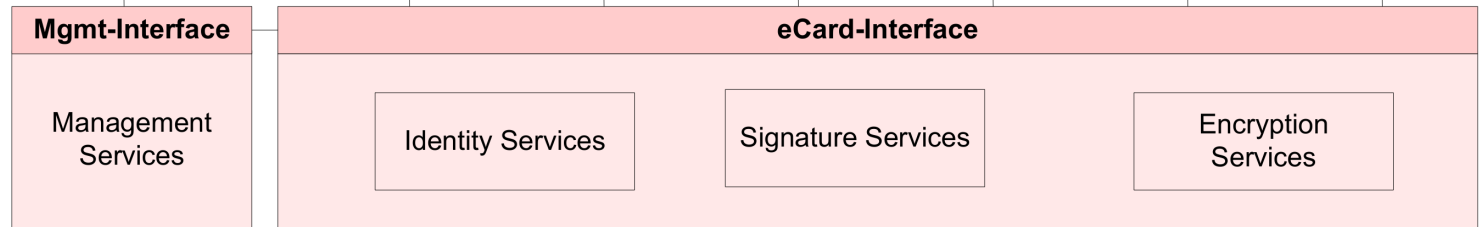


# eCard-API Architecture

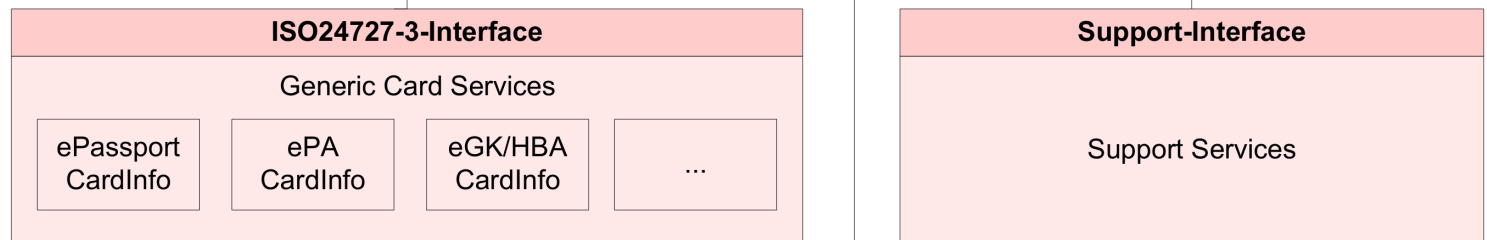
## Application-Layer



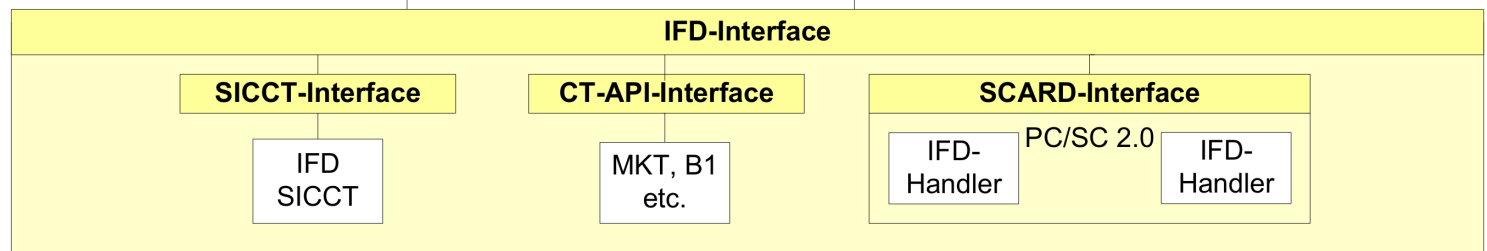
## Identity-Layer



## Service-Access-Layer



## Terminal-Layer





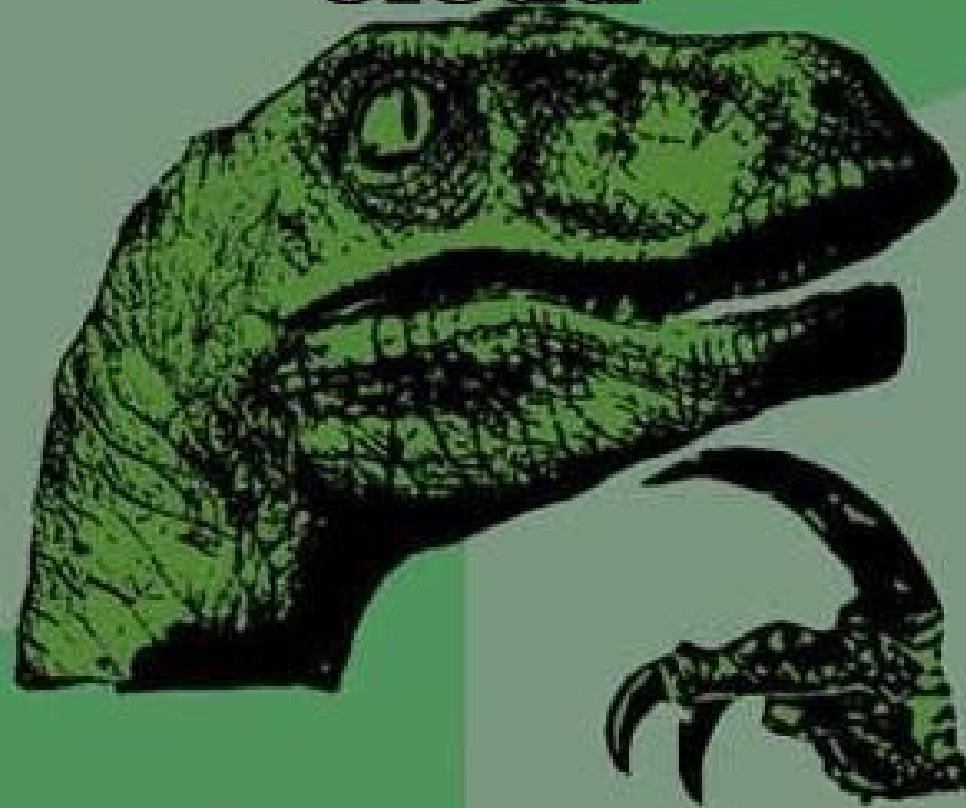
# Agenda

- Introduction
  - Identity Management
  - eCard-API-Framework
- SkIDentity
- Open eCard App
- Summary



Identity + Cloud = SkIDentity

**Is my identity in the  
cloud**



**a SkIDentity?**



# Who is SkIDentity?

Supported by:



Federal Ministry  
of Economics  
and Technology

on the basis of a decision  
by the German Bundestag

Trusted  Cloud

 SkIDentity





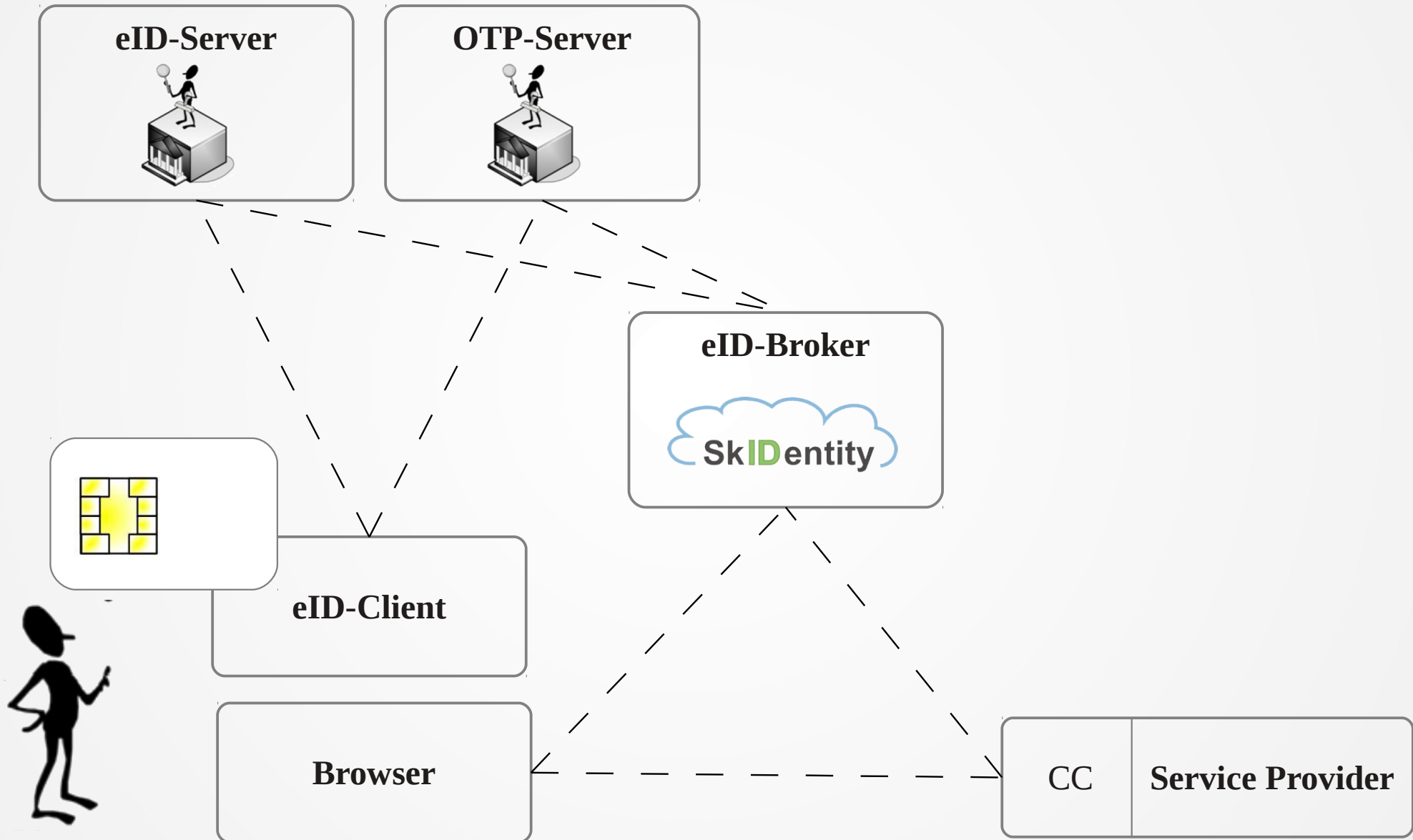
# Goals of SkIDentity

- Create infrastructure with all components
  - Cloud Connector
  - Multi Protocol IdP
  - eID-Server backends
  - Client Application for arbitrary HW-Tokens
- Make infrastructure easy to use (for SP)
- Combine multiple identities/providers
- Make it easy enough for users to use and *accept* HW-Tokens





# Architecture





# How could it look like?



**Sign in with twitter**



**Sign in with facebook**

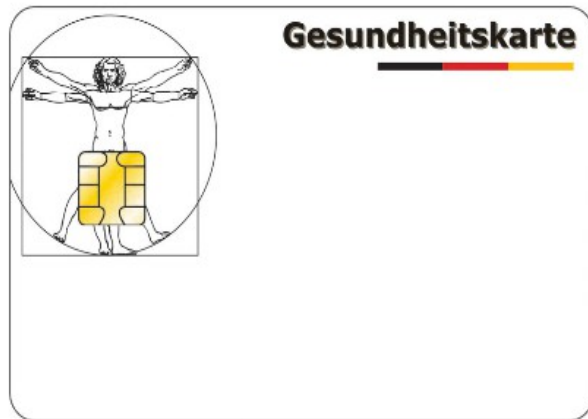


**Sign in with SkIdentity**



# What happens next?

- Token selection



SCM Microsystems Inc. SCR 335 [CCID Interface] (21120945304956) 00 00



REINER SCT cyberJack RFID basis 01 00

- To be continued ...



# Benefits

- Supports multiple protocols
  - When e.g. OAuth is integrated, the SP can switch the IdP, or support multiple IdPs
- More tokens supported by enabling the appropriate backend and add a CardInfo file
- Much easier to integrate than  $n$  eID-Servers
- Anonymous identities with Site-specific Pseudonyms



# Agenda

- Introduction
  - Identity Management
  - eCard-API-Framework
- SkIDentity
- Open eCard App
- Summary



# Existing eCard Clients

Identitätsnachweis - Angefragte Daten

Anbieterinformationen

**Angefragte Daten**

PIN-Eingabe

Übermittlung

Angefragte Daten

Für den genannten Zweck bitten wir Sie, die folgenden Daten aus Ihrem Personalausweis zu übermitteln

[Datenschutzerklärung](#)

|                                                |                                                    |
|------------------------------------------------|----------------------------------------------------|
| <input checked="" type="checkbox"/> Vorname(n) | <input type="checkbox"/> Ordens- oder Künstlername |
| <input checked="" type="checkbox"/> Name       | <input type="checkbox"/> Ausweistyp                |
| <input type="checkbox"/> Doktorgrad            | <input type="checkbox"/> Ausstellendes Land        |
| <input checked="" type="checkbox"/> Anschrift  | <input type="checkbox"/> Wohnortbestätigung        |
| <input type="checkbox"/> Geburtstag            | <input type="checkbox"/> Altersverifikation        |
| <input type="checkbox"/> Geburtsort            | <input type="checkbox"/> Pseudonym / Kartenkennung |

Wenn Sie mit der Übermittlung der ausgewählten Daten einverstanden sind, geben Sie bitte Ihre 6-stellige Personalausweis-PIN ein.

Personalausweis-PIN

Bildschirmtastatur

Zurück Weiter Abbrechen

Der neue Personalausweis  
Meine wichtigste Karte.

Wählen Sie zum Übertragen der Daten die entsprechende Schaltfläche. Sie werden dann in einem neuen Fenster aufgefordert, Ihre persönliche Identifikationsnummer (PIN) einzugeben.

a a a

← × →

AGETO Service GmbH - nPA Client

**AGETO**

Zertifikat des Diensteanbieters

**SYNCHRONITY GmbH**  
<https://www.synchronity.net/demoportal/>  
Gültigkeit: 31.05.2011 - 02.06.2011

Name, Anschrift und E-Mail-Adresse des Diensteanbieters:  
SYNCHRONITY GmbH  
Winklerstr. 2  
07745 Jena  
[npa@synchronity.de](mailto:npa@synchronity.de)

Aussteller des Berechtigungszertifikates

**D-Trust GmbH**  
<http://www.d-trust.net>

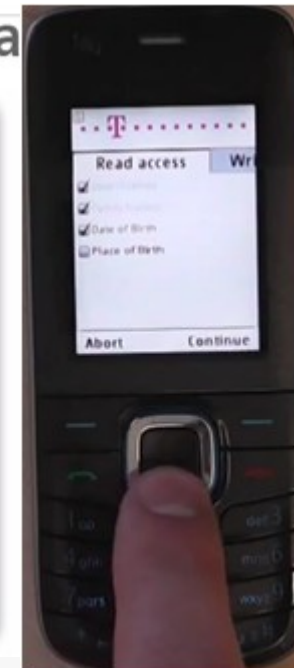
Auszulesende Daten

|                                                  |                                                               |
|--------------------------------------------------|---------------------------------------------------------------|
| <input checked="" type="checkbox"/> Vorname(n)   | <input type="checkbox"/> Ordens- und Künstlername             |
| <input checked="" type="checkbox"/> Name         | <input type="checkbox"/> Ausweistyp                           |
| <input checked="" type="checkbox"/> Doktorgrad   | <input type="checkbox"/> Ausstellendes Land                   |
| <input checked="" type="checkbox"/> Anschrift    | <input type="checkbox"/> Wohnortbestätigung                   |
| <input checked="" type="checkbox"/> Geburtsdatum | <input type="checkbox"/> Altersverifikation                   |
| <input type="checkbox"/> Geburtsort              | <input checked="" type="checkbox"/> Pseudonym / Kartenkennung |

Personalausweis-PIN

Bestätigen Abbrechen

Warte auf PIN-Eingabe.





# What is the problem?

- None has publicly available source
- All free (beer) clients are limited to nPA
- No client has real CardInfo support
- eCard-API is still changing, new features get adopted quite slowly
- Clients in general not non-Web-SSO ready
- Ports to other platforms
- Clients only support Auth and Sign
- ...



# Open eCard App - The Facts!

- Dual license (GPLv3 or proprietary)
- Heavily modularized to support pluggable architecture
- Multiple application bundles
- Lightweight design
- Extensible
  - Protocols
  - Frontend interface (binding)
  - Builtin protocol endpoints
  - User Consent GUI



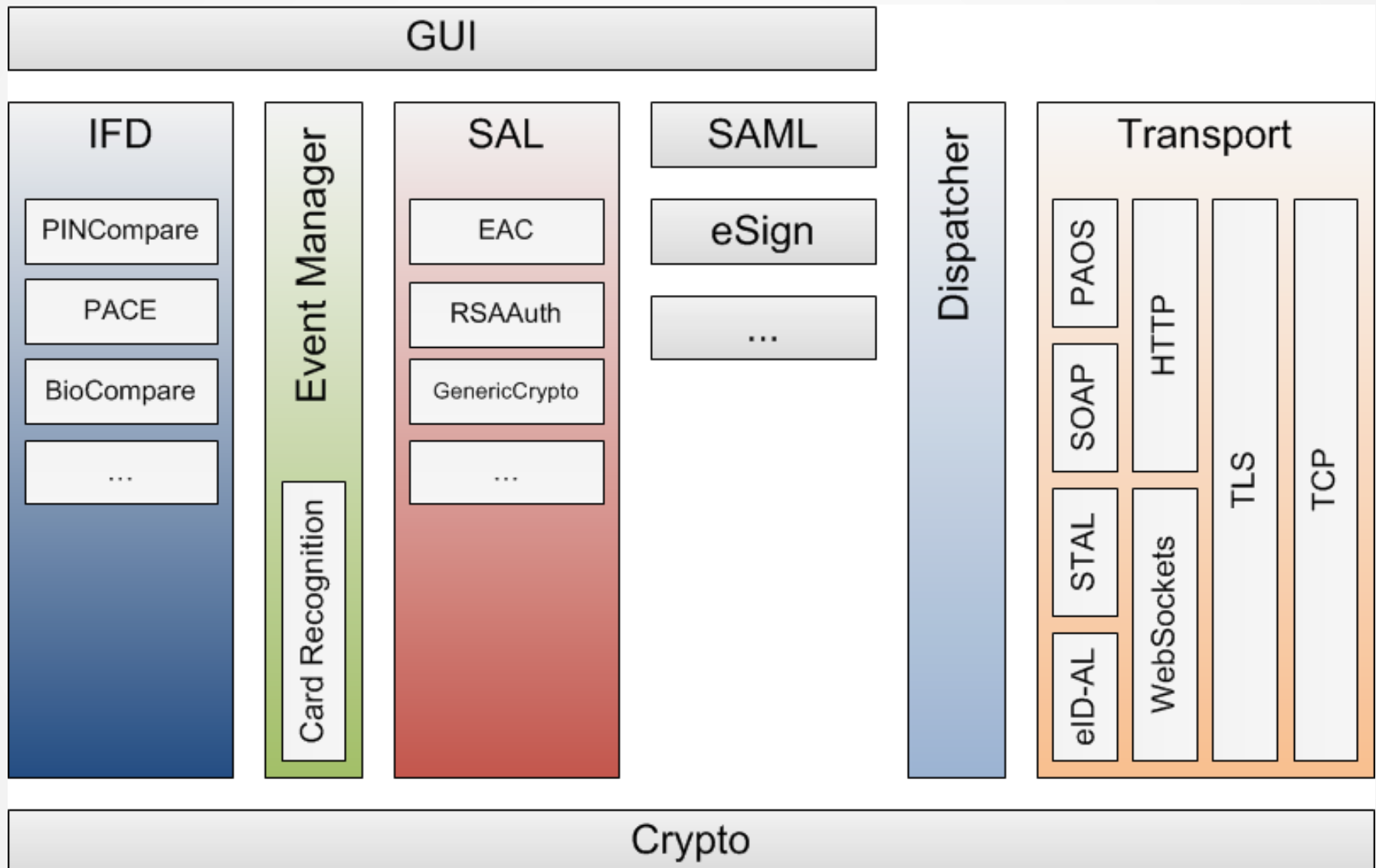


# Technical Basis

- Libraries
  - Java integrated
    - JAXB, SmartcardIO, Android NFC, ...
  - Bouncycastle
  - slf4j
- Clients in the first release
  - Rich Client for Desktops
  - Applet
  - Android



# High-Level Design





# User Consent Screenshots


**Anbieter**  
Angefragte Daten  
PIN-Eingabe

**Anbieter**  
  
Über den Diensteanbieter und seine Berechtigung liegen folgende Information vor. Bitte überprüfen Sie, dass Name und Internetadresse mit dem gewünschten Diensteanbieter übereinstimmen.  
  
**Name**  
mtG eID-Server  
  
**Internetadresse**  
<http://www.mtg-eID-Server.de>  
  
**Nutzungsbestimmungen**   
  
**Gültigkeit**   
  
**Aussteller des Berechtigung**   
  
**Internetadresse des Ausstellers**

**Weiter** **Abbrechen**



# User Consent Screenshots



Anbieter

Angefragte Daten

PIN-Eingabe

## Identitätsnachweis

Angefragte Daten

Der Anbieter mtG eID-Server fordert folgenden Daten von Ihnen an:

|                                                        |                                                        |
|--------------------------------------------------------|--------------------------------------------------------|
| <input checked="" type="checkbox"/> Ausweistyp         | <input checked="" type="checkbox"/> Ausstellendes Land |
| <input checked="" type="checkbox"/> Ablaufdatum        | <input checked="" type="checkbox"/> Vorname            |
| <input checked="" type="checkbox"/> Nachname           | <input checked="" type="checkbox"/> Künstlername       |
| <input checked="" type="checkbox"/> Akademischer Titel | <input checked="" type="checkbox"/> Geburtstag         |
| <input checked="" type="checkbox"/> Geburtsort         |                                                        |

**Hinweis**  
Die markierten Elemente benötigt der Anbieter zur Durchführung seiner Dienstleistung. Optionale Daten können Sie hinzufügen.

Zurück

Weiter

Abbrechen



# User Consent Screenshots

**Identitätsnachweis**



Anbieter

Angefragte Daten

**PIN-Eingabe**

**PIN-Eingabe**

Durch die Eingabe Ihrer PIN bestätigen Sie, dass folgende Daten an den Diensteanbieter übermittelt werden:

♥ Geburtstag


PIN

Zurück Bestätigen Abbrechen



# PIN-entry from IFD

PACE Protocol



**PIN-Eingabe**

**PIN-Eingabe**

Zur Durchführung der Operation geben Sie bitte Ihre PIN ein.

PIN

**Weiter** **Abbrechen**



# Current Status and Roadmap

- Complete Features
  - Dispatcher, Recognition and Event Engine, GUI
- Almost Complete Features
  - IFD, SAL, CardInfo support
- Milestone 1.0.0-pre1
  - Feature development of EAC and TLS protocols
- Milestone 1.0.0-pre2
  - Documentation and Testing
- Release 1.0.0
  - Finish Rich Client, Applet and Android app



# Participate

- Source will be on GitHub
- What can you do?
  - Explore the code and find bugs
  - Activation Request Dispatcher
  - PKCS12 module
  - Nice Qt/GTK GUI
  - smart-card Inspector
  - ... or become part of our team and work on the beefy stuff





# Agenda

- Introduction
  - Identity Management
  - eCard-API-Framework
- SkIDentity
- Open eCard App
- Summary

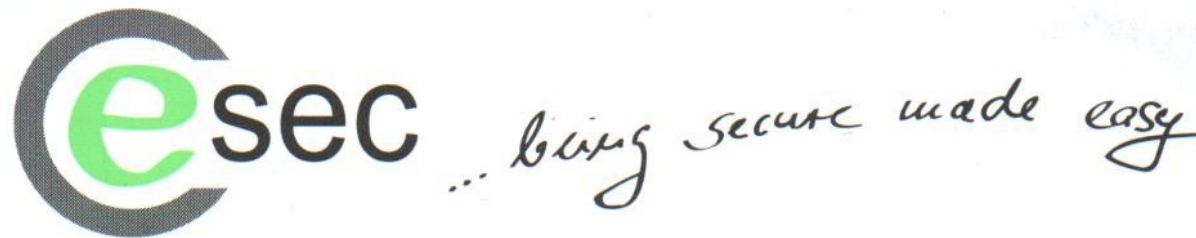


# Summary

- Using Hardware-Tokens
  - prevents most common attacks
  - increases privacy
- With a free OSS App, anybody can
  - find and report bugs
  - create custom applications
- SkIDentity + Open eCard App
  - makes strong identities usable



# Thank you for your kind attention!



**ecsec GmbH**

Sudetenstr. 16  
96247 Michelau, Germany  
mob. + 49 176 21845766  
tobias.wich@ecsec.de  
<http://www.ecsec.de>

Dipl.-Inf. (FH)

**Tobias Wich**

Senior Consultant