ecsec ... bring secure made easy

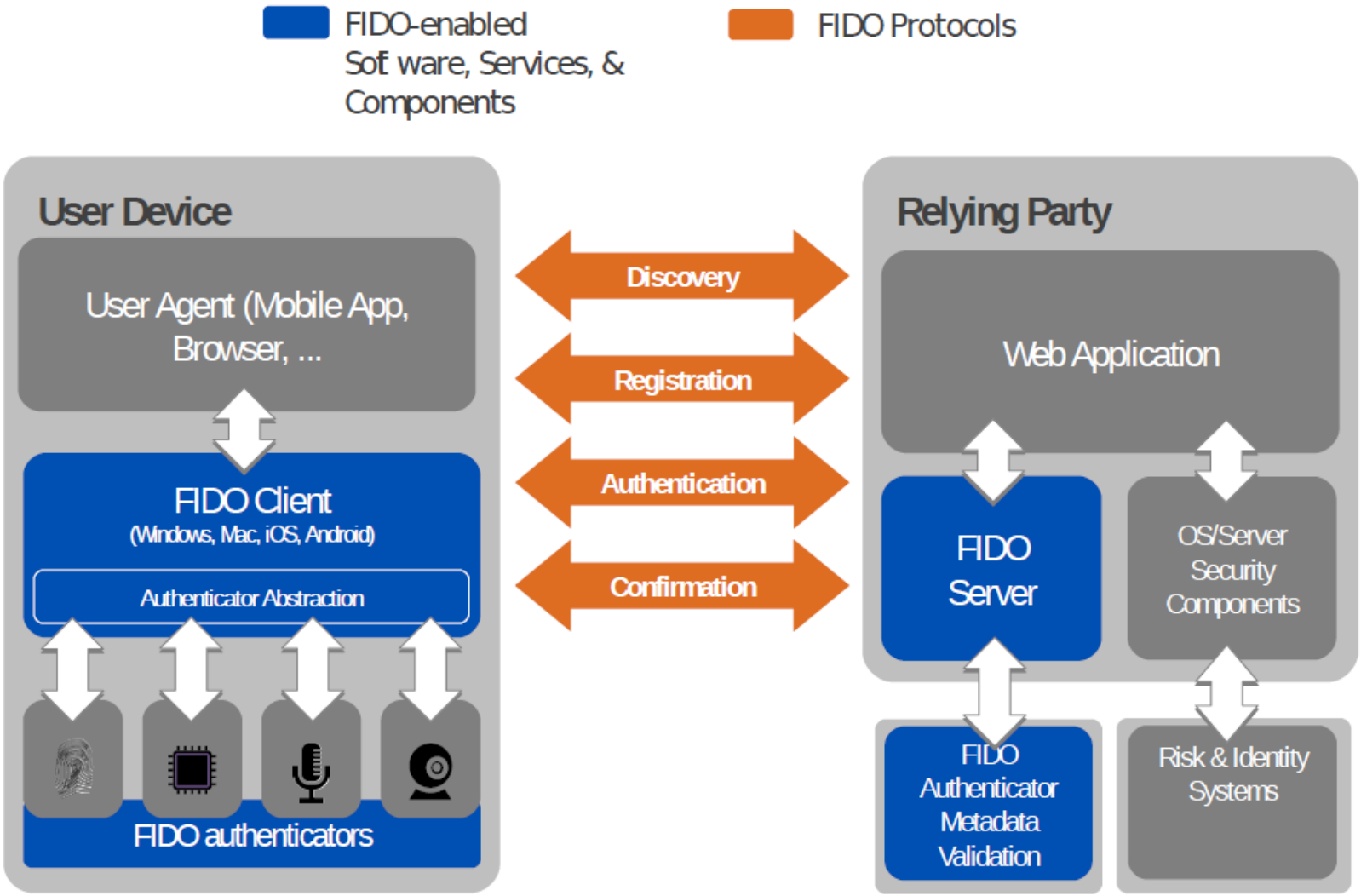
Towards harmonizing ISO/IEC 24727 with FIDO and Web Crypto API

Dr. Detlef Hühnlein

Agenda

- FIDO
- ISO/IEC 24727
- Web Crypto API

FIDO Universal Authentication Framework (UAF)

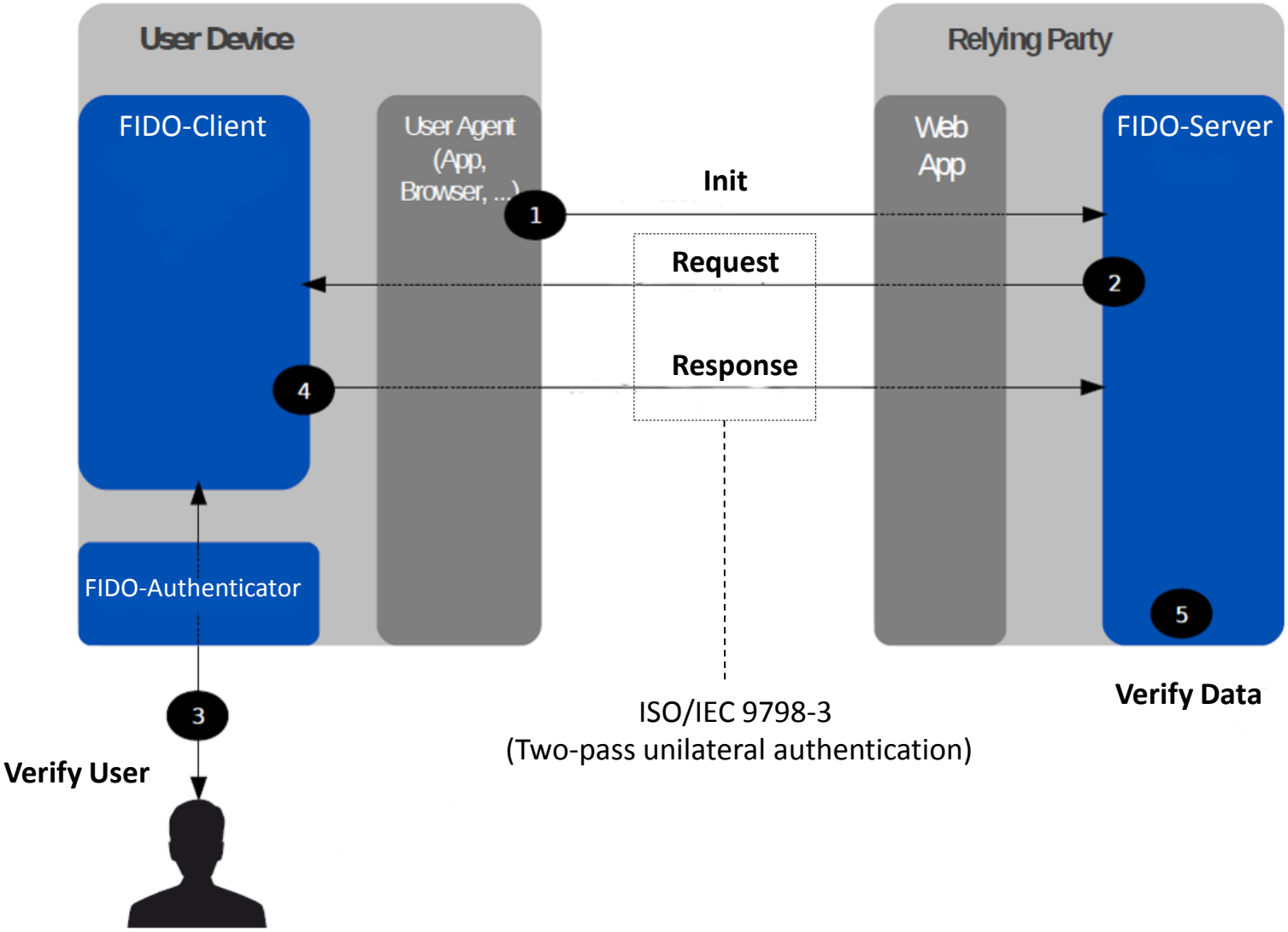


FIDO Discovery

To discover if the user's client software and devices support UAF and if Authenticator capabilities are available that it may be willing to accept for authentication, Relying Party code in the browser can use the following interface.

```
interface Discovery {
    readonly attribute Version[] supportedUAFVersions;
    readonly attribute DOMString clientVendor;
    readonly attribute Version clientVersion;
    readonly attribute Authenticator[] availableAuthenticators;
    void checkPolicy(DOMString message, ErrorCallback cb);
}
```

FIDO Protocol Outline (Registration/Authentication/Confirmation)



Agenda

- FIDO
- ISO/IEC 24727
- Web Crypto API

ISO/IEC 24727 – Identification Cards

e.g. Personal Identity Verification (PIV)

e.g. European Citizen Card (ECC)

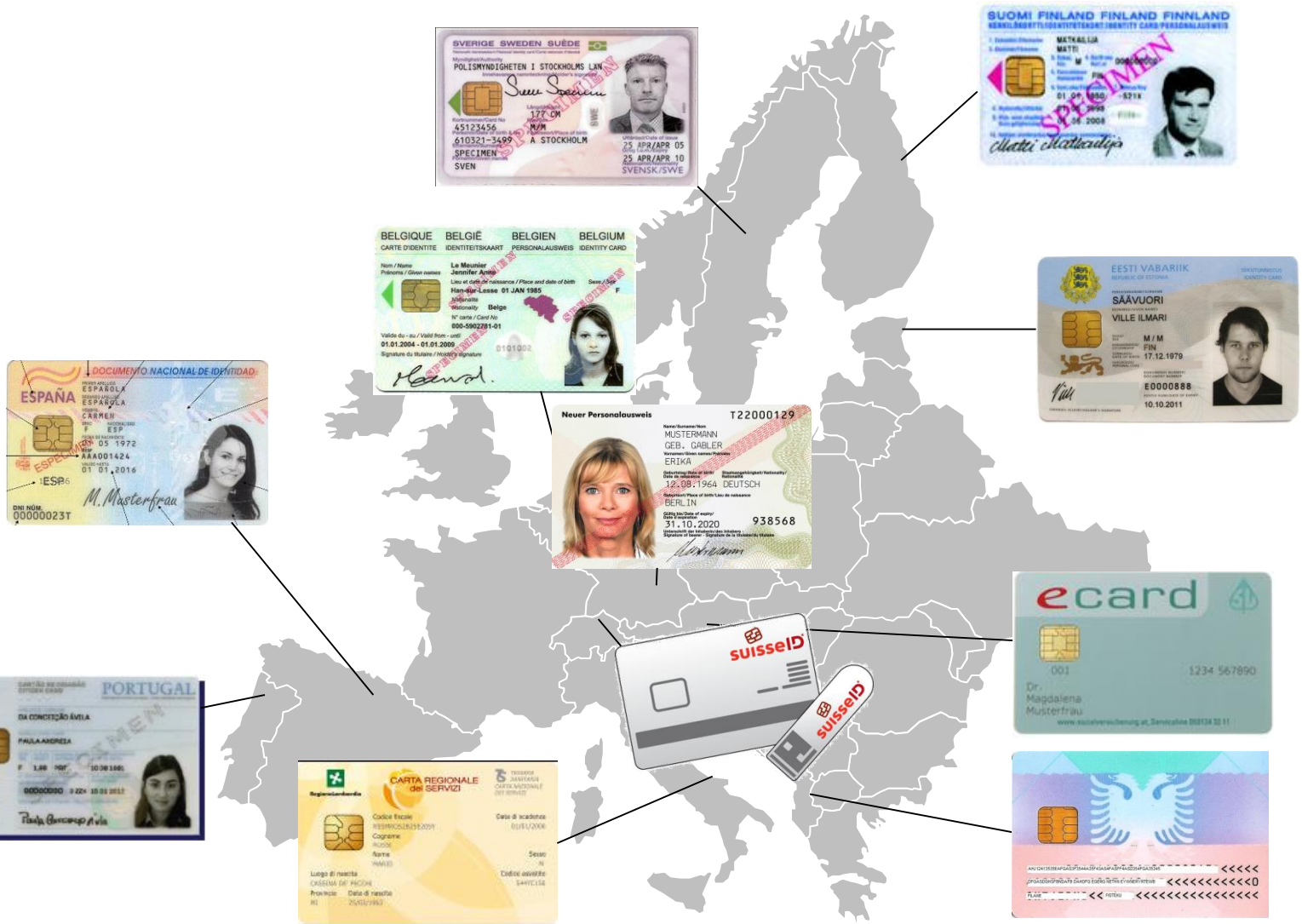
e.g. Malaysia

e.g. Nigeria

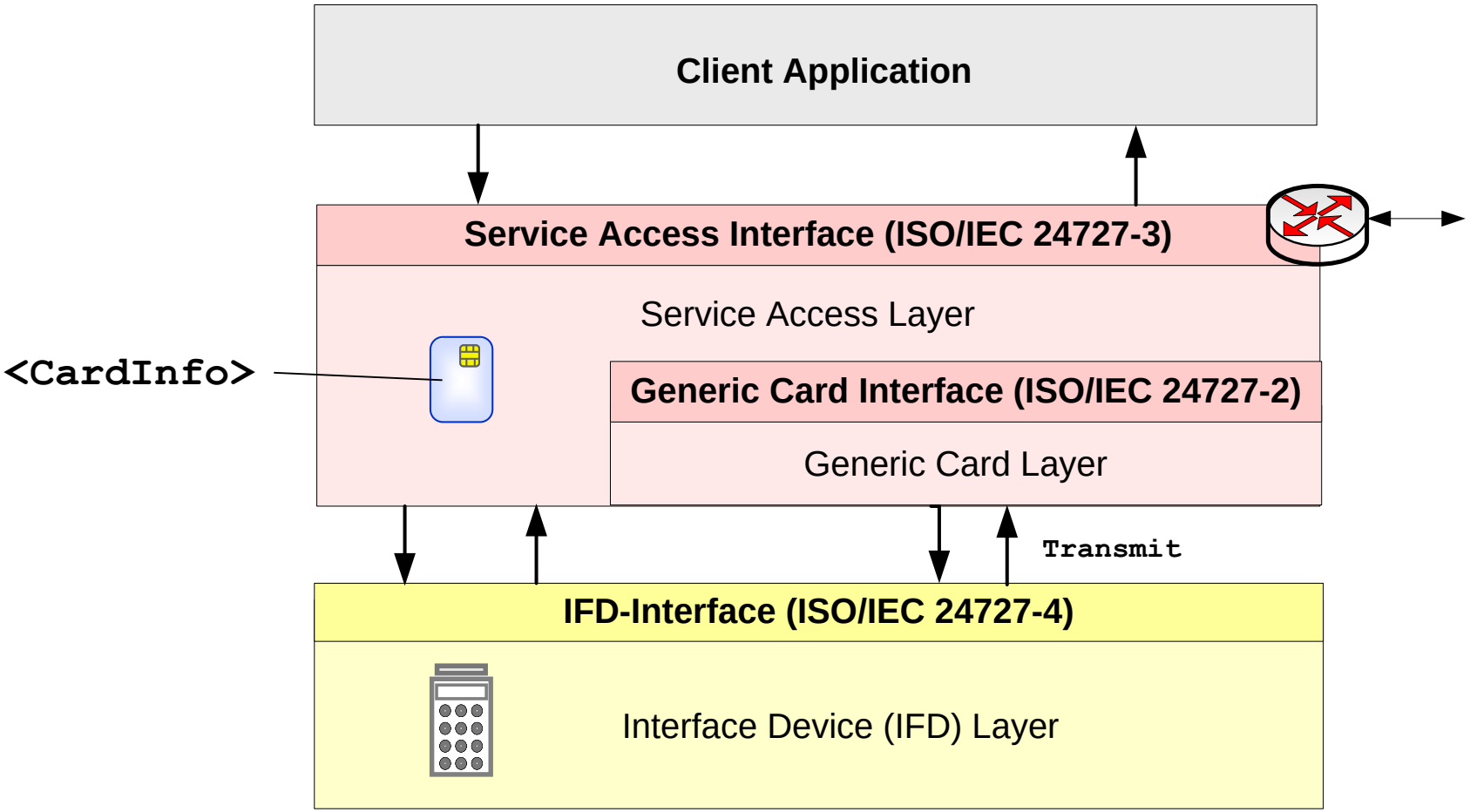
e.g. Brasil, Peru

e.g. Australian Drivers License

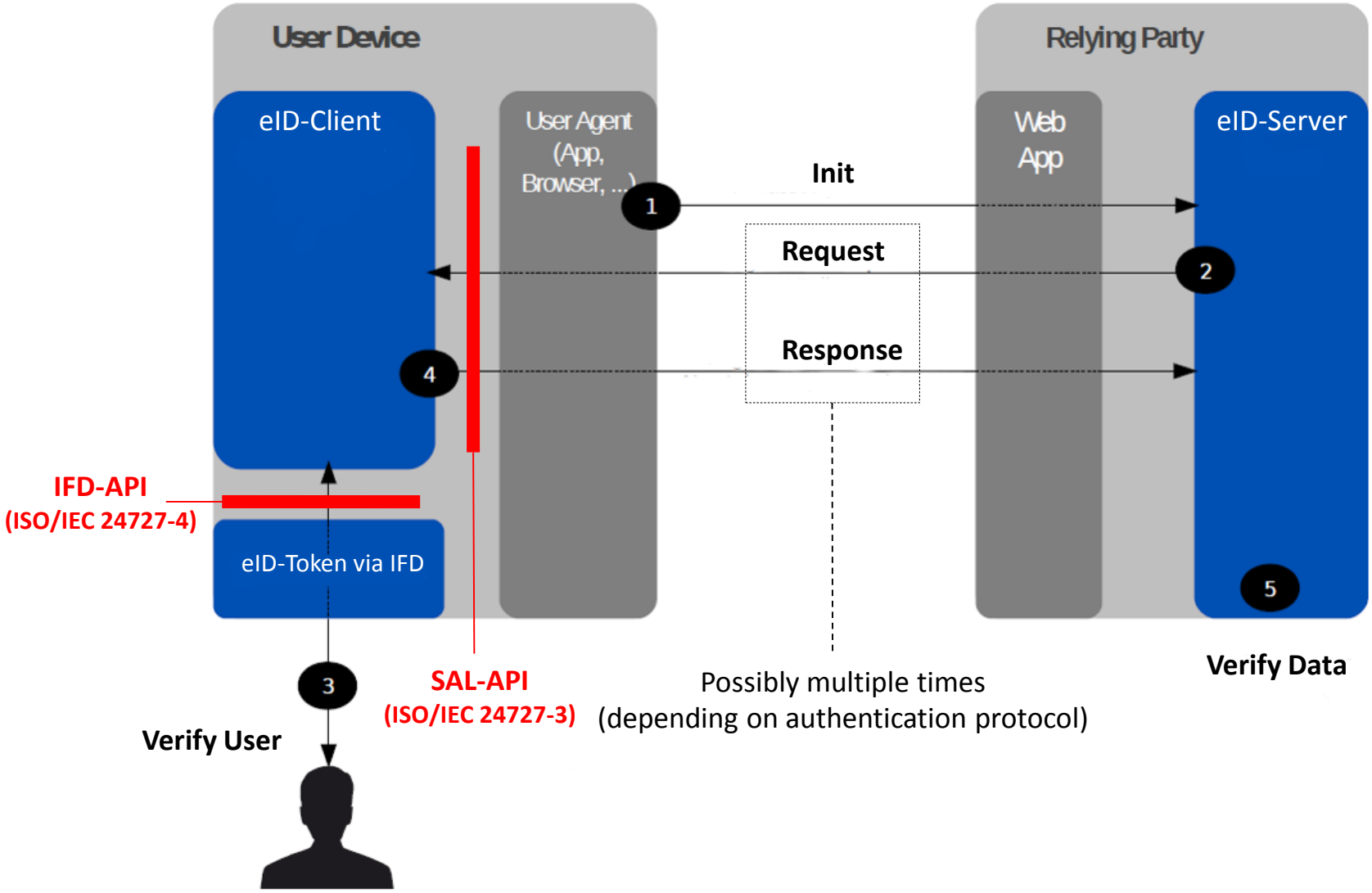
Identification Cards in Europe



ISO/IEC 24727 Architecture



ISO/IEC 24727 Protocol Outline



ISO/IEC 24727-4 (IFD-API)

- Card terminal functions
  - EstablishContext
  - ReleaseContext
  - ListIFDs
  - GetIFDCapabilities
  - GetStatus
  - Wait
  - Cancel
  - ControlIFD
- Channel Functions
  - EstablishChannel
  - DestroyChannel
- Card functions
  - Connect
  - Disconnect
  - BeginTransaction
  - EndTransaction
  - Transmit
- User interaction functions
  - VerifyUser
  - ModifyVerificationData
  - Output
- IFD-Callback-Interface
  - SignalEvent

http://ws.openecard.org/schema/ISOIFD.wsdl

ISO/IEC 24727-3 (Service Access Layer)

- Card-application-service Access
  - Initialize
  - Terminate
  - CardApplicationPath
- Connection-service
  - CardApplicationConnect
  - CardApplicationDisconnect
  - CardApplicationStartSession
  - CardApplicationEndSession
- Card-application service
  - CardApplicationList
  - CardApplicationCreate
  - CardAppicationDelete
  - CardApplicationServiceList
  - CardApplicationServiceCreate
  - CardApplicationServiceLoad
  - CardApplicationServiceDelete
  - CardApplicationServiceDescribe
  - ExecuteAction
- Named data service
  - DataSetList
  - DataSetCreate
  - DataSetSelect
  - DataSetDelete
  - DSIList
  - DSICreate
  - DSIDelete
  - DSIRead
  - DSIWrite
- Cryptographic service
  - Encipher
  - Decipher
  - GetRandom
  - Hash
  - Sign
  - VerifySignature
  - VerifyCertificate
- Differential-identity service
  - DIDList
  - DIDCreate
  - DIDGet
  - DIDUpdate
  - DIDDelete
  - DIDAuthenticate
- Authorization service
  - ACLList
  - ACLModify

http://ws.openecard.org/schema/ISO24727-3.wsdl

ISO/IEC 24727 Discovery

http://127.0.0.1:24727/getStatus

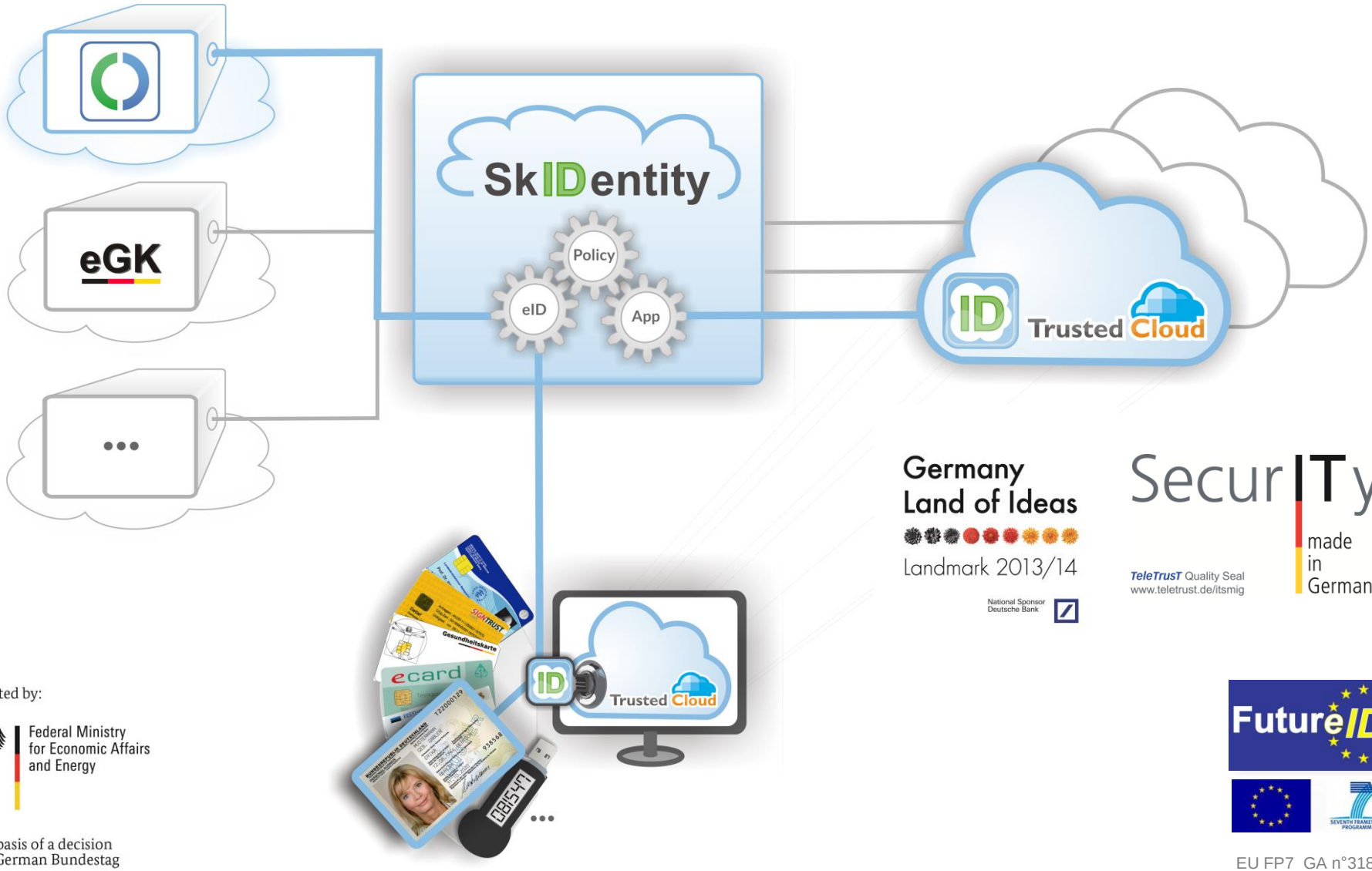
```
<Status>
    <ConnectionHandle/> *
    <UserAgent/>
    <SupportedAPIVersions/> *
    <SupportedCards>
          <CardType/>
          <DIDProtocols/> ?
     </SupportedCards> *
     <SupportedDIDProtocols/> *
     <AdditionalFeatures/> ?
</Status>
```

http://127.0.0.1:24727/waitForChange?session=...

```
<StatusChange>
    <ConnectionHandle/>
    <Action/>
</StatusChange>
```

https://dev.openecard.org/projects/open-ecard/wiki/Control_Interface

SkIDentity – Trustworthy Identities as a Service



Germany Land of Ideas
Landmark 2013/14
National Sponsor Deutsche Bank

SecurITy made in Germany
TeleTrusT Quality Seal
www.teletrust.de/itsmig

Supported by:
Federal Ministry for Economic Affairs and Energy
on the basis of a decision by the German Bundestag

FutureID
EU FP7 GA n°318424

Agenda

- FIDO
- ISO/IEC 24727
- Web Crypto API

Conclusion and recommendations for Web Crypto API

- FIDO and ISO/IEC 24727
  - support both strong authentication
  - ISO/IEC 24727 is slightly more powerful as it allows to support arbitrary eID cards and authentication protocols
  - should be considered for Web Crypto API extension
- Recommendations for Web Crypto API
  - Introduce discovery mechanism (cf. GetStatus, WaitForChange)
  - Introduce protocol agnostic `Authenticate` function (and framework for adding authentication protocols)
  - Implementations may build upon existing Open Source ISO/IEC 24727 stack (see http://openecard.org)

Thank you very much for your kind attention!

Trusted Cloud

Germany Land of Ideas
Landmark 2013/14
National Sponsor Deutsche Bank

Contact