



# World wide standardisation in electronic ID, an overview

**Jan van Arkel**

Co-Chairman eEurope Smart Card Charter  
Ambassador CEN/ISSS WS eAuthentication

ePoch 3 Conference, June 7, Dusseldorf



# Standardisation of eID/eAut

- 2 European groups
- 1 ISO group
- 1 joint EU, Japan, US initiative



# Europe

## CEN/ISSS WS eAuthentication

(Government requirements, architectural model, Business models, Legal Framework, Card issuer guidelines, Human interface aspects, Multi-application environment, eID policy vision)

## CEN 224 WG 15 European Citizen Card

( Policy and rules for CMS, Physical and logical card characteristics, data elements and structures, IAS procedures, Test methods)



# Status of WS eAut

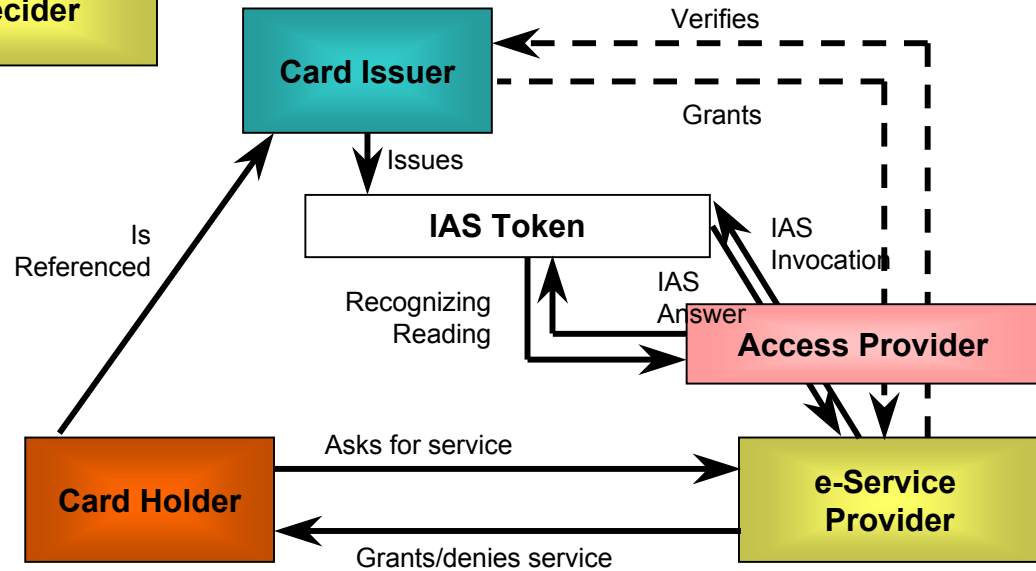
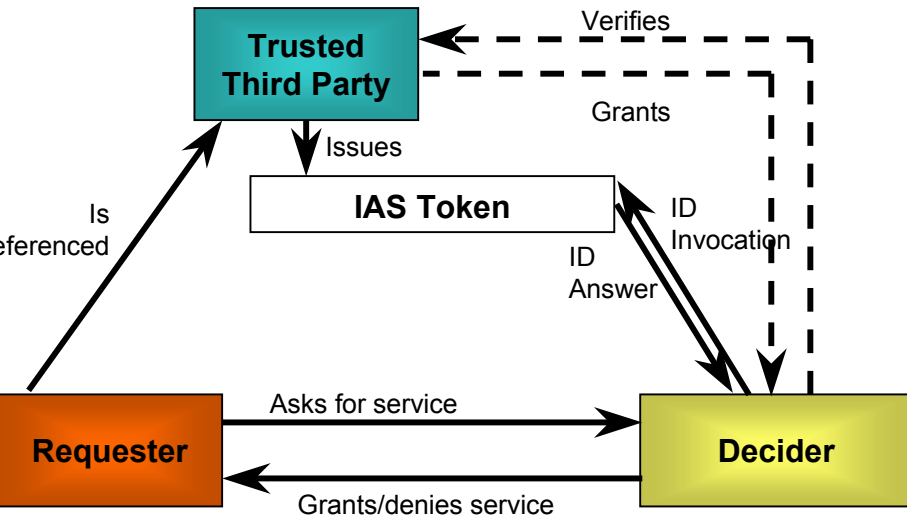
- Kick off meeting on September 16, 2003
- 38 registered participants, 75 interested people on mailing list
- Chair: Theo van Sprundel, Axalto
- Secretariat: Catherine Protic, AFNOR
- Project Team of 7 experts appointed in January 2004
- Plenary on March 10, 2004
- Draft CWA is due for July 2004;
- WP 4 Draft Vision document is available



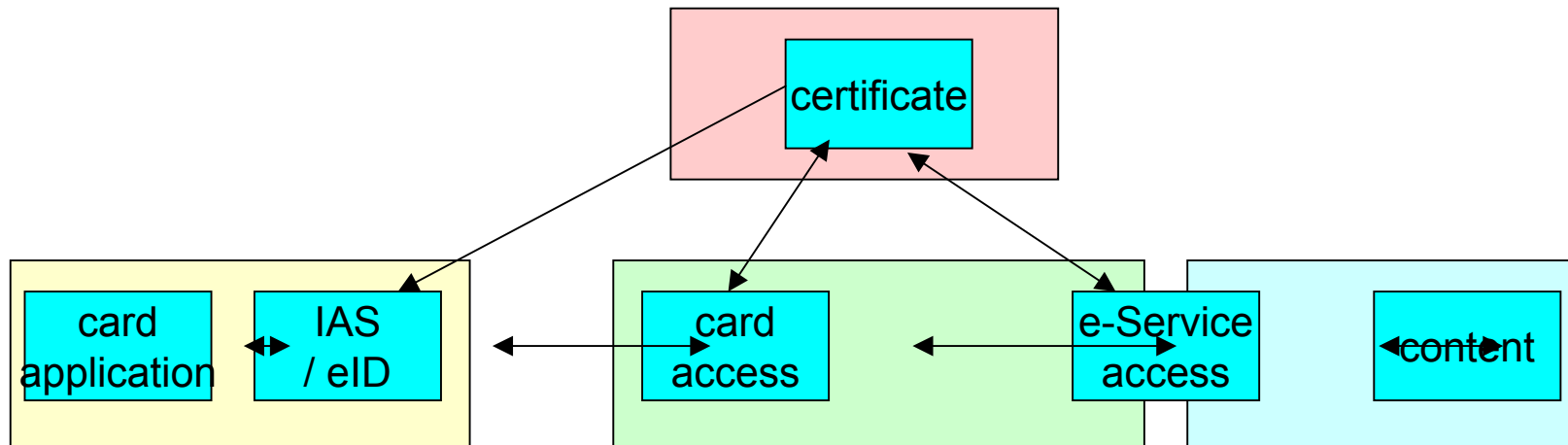
# Status of WS eAut

- Common requirements setting meeting July 6, 2004
- Next plenary on September 20, 2004
- Final CWA for voting Q 3 2004
- Envisioned closing of WS early 2004

# eID and the trust model

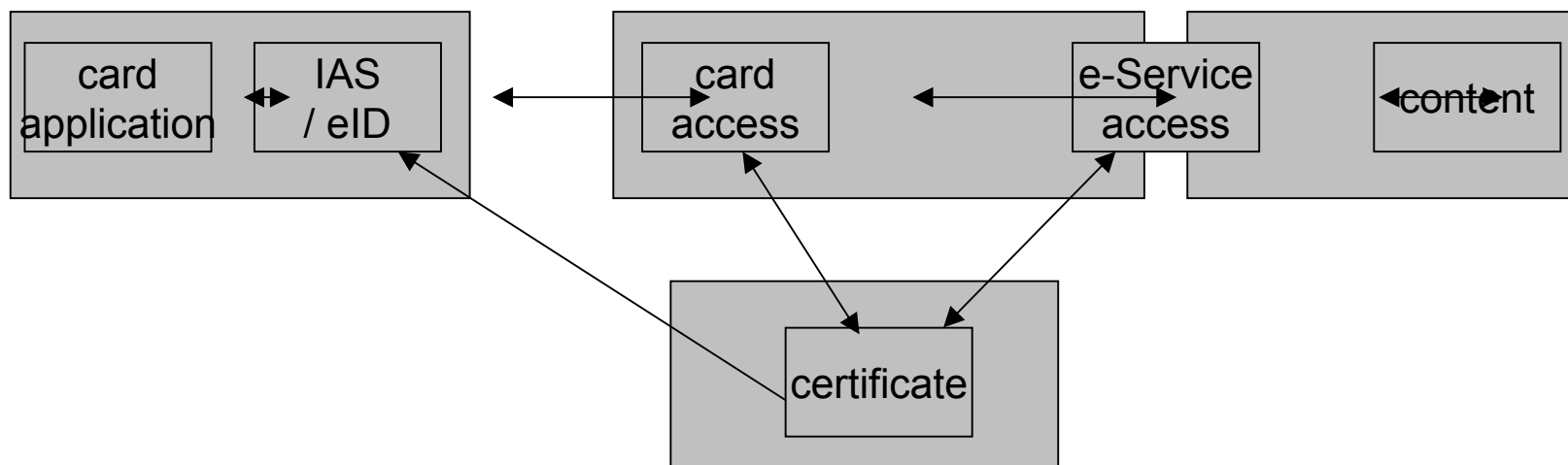


# Closed eID scheme

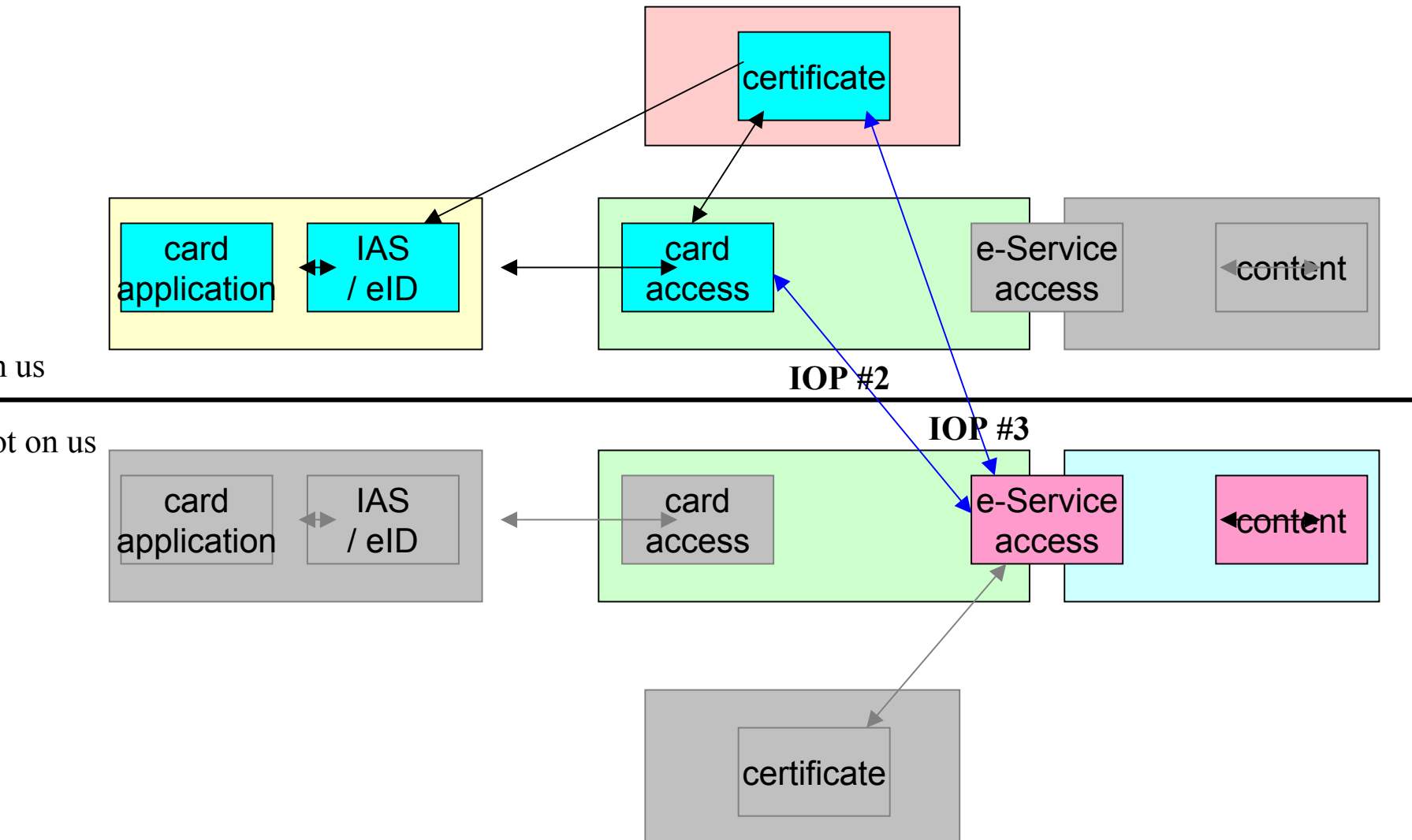


n us

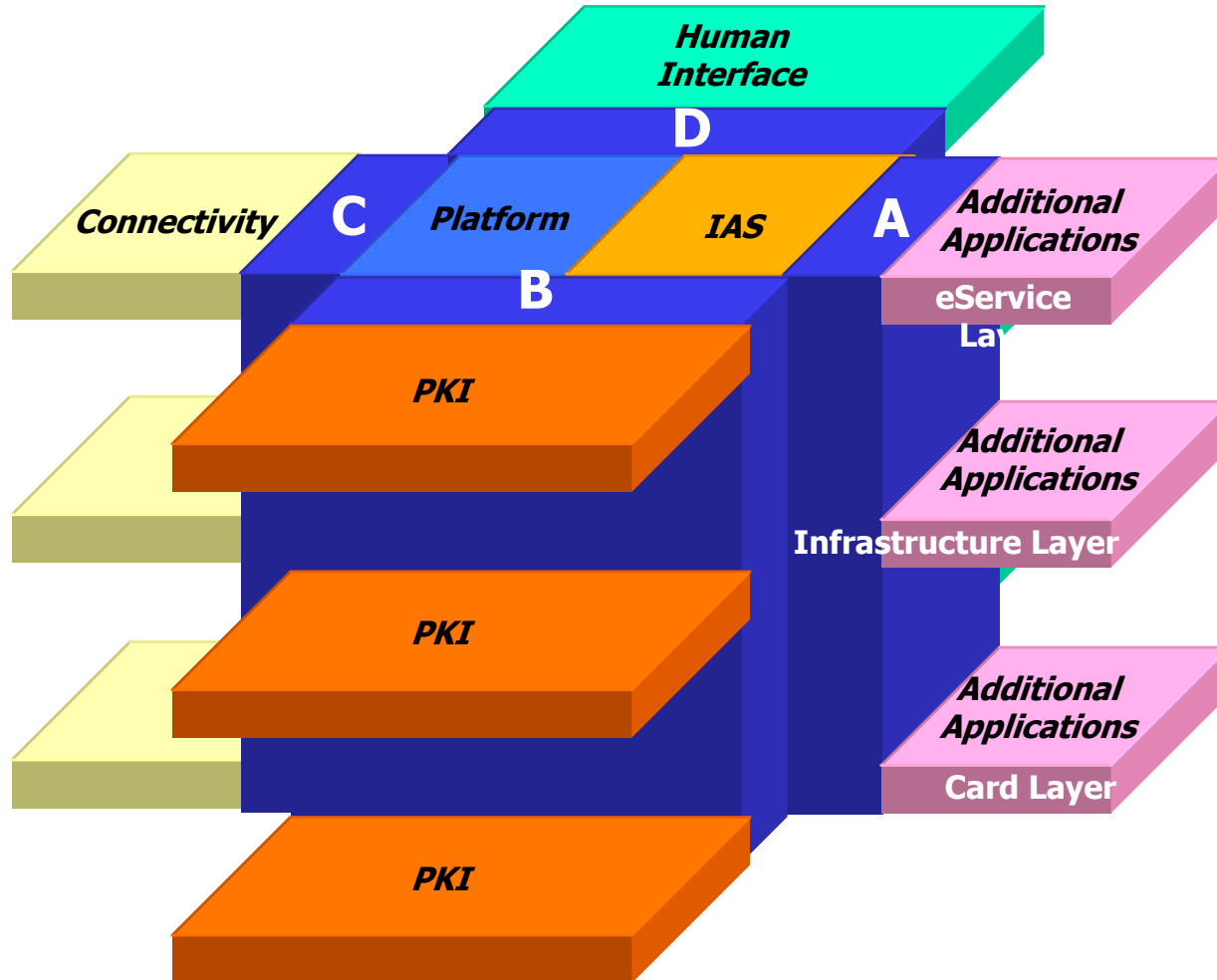
ot on us



# eService interoperability



# Functional Model



# The Electronic Citizen Card Scope

- **Description of basic and additional services supported**
- **Policy and rules for ECC management and operation**
- **Physical and electrical Characteristics**
- **Security features & options**
  - Physical layout
  - Card durability
  - Electrical characteristics for contact and/or contactless interfaces
- **Logical characteristics**
- **Data elements and data structures**
  - Access to Data
  - Access to Services
  - Security mechanisms (Integrity, Confidentiality, Authentication and Non-repudiation)
  - Security profiles
- **Identification, Authentication and Signature procedures**
- **Card and application Life cycle management**
- **Test methods**
  - Physical
  - Logical
- **Examples of SERVICES that can be supported by the ECC (informative)**
- **Registration and delivery procedures (informative)**



# Status of CEN 224 –WG 15 ECC

- Workgroup was launched in Feb 2004
- Chair: Lorenzo Gaston, Axalto, Secretariat: tbd
- Constituency: 20+ organisations
- 2 Subgroups for Electronic data and for Physical aspects
- SG 1 has defined up a detailed table of content for Electronic Data and Functions in its first meeting
- WG 15 Plenary was held on 4-5 May 2004
- Requirements setting meeting on July 6, 2004
- Next SG 1 and 2 meetings on July 7, 2004
- Follow up plenary and SG's in October 2004
- Draft Technical standard due in Q 1 2005



# Subgroup 1, logical & electronical aspects

## Condensed table of content

- Preface
- Scope
- Logical Data
- Data elements and data structures
- Access to data objects
- Access to files (native/multiapplication context)
- Implementation of card services including algorithms/references
- Access to card services
- Security profiles / Use cases



# Subgroup 1, logical & electronical aspects

- Annex 1) Card life cycle
- Annex 2) Personalisation aspects
- Annex 3) Public Key Infrastructure considerations
- Annex 4) Card-Terminal negotiation of security level / Risk management
- Annex 4.1 Examples of use cases
- Annex 5) Test plans/performance requirements



# CEN 224 – 15 Subgroup 2 physical aspects

- Subgroup 2 has been launched in the Copenhagen meeting. A call for SG2 leader is out.  
L. Gaston shall be acting for the first SG2 meeting
- SG2 shall develop the part of the standard dealing with the physical characteristics and electrical interface of the ECC



# ISO SC 17

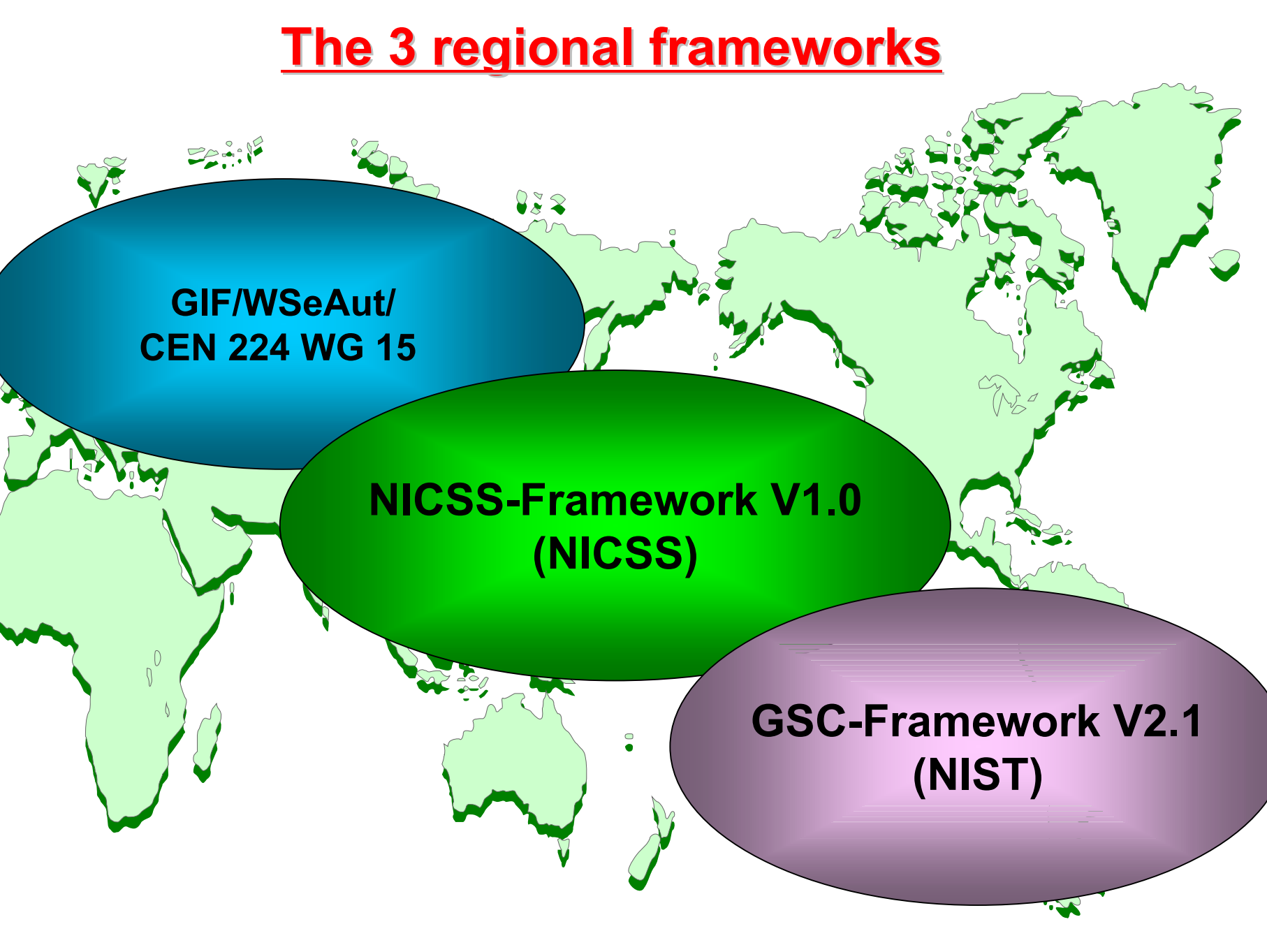
- ❑ ISO SC 17 WG 4, TF 9 established March 5, 2004 following a proposal initiated by NIST (GSC-IS Spec)
- ❑ Title: Application Programming Interfaces for Integrated Circuit Card (API-ICC)
- ❑ Scope: Standardization of a set of structured programming interfaces for interactions between integrated circuit cards and external applications to include generic services for multi-sector use



# ISO SC 17

- ❑ Expected output:  
new SC standard ISO 24727
- ❑ TF 9 call for experts is (still) open
- ❑ Call for contributions is open till June 30
- ❑ Aggressive scheme, 1-2 years
- ❑ Even more aggressive scheme, US  
national standard, 1 year

# The 3 regional frameworks

A world map with a light green background and dark green outlines for continents. Three overlapping ovals are placed over the map: a blue oval over North America, a green oval over Europe and Africa, and a purple oval over Asia and Australia. Each oval contains text identifying a regional framework.

**GIF/WSeAut/  
CEN 224 WG 15**

**NICSS-Framework V1.0  
(NICSS)**

**GSC-Framework V2.1  
(NIST)**



# Objective of the Global Collaboration Forum on IAS

- Define common core for global IAS interoperability in Smart Card domain
- Have this core standardised as part of the ISO/IEC 7816- series
- Action for adding post issuance loading/deleting commands in ISO 7816 (in progress, NWI leading to ISO 7816 - 13)



# Status of Global Collaboration Forum on IAS

- ❑ Participants: eESC, NICSS, NIST, Global Platform, Maosco
- ❑ Regular 6 monthly meetings (in conjunction with CTST and CARTES)
- ❑ NIST has chair at present
- ❑ Products so far:
  - Mapping document of GIF/GSC-IS and NICSS Framework
  - Draft for common Glossary of terms
  - First draft for Common Requirements for eID in eGovernment domain



# **Common requirements for Electronic ID in eGovernment version 0.6, June 5, 2004**



# Scope & basic concepts

The positioning is interoperable electronic ID and eAuthentication in the global eGovernment domain

The concept is based on the Smart Card (in contact and contactless mode) as the supporting token for eAuthentication as well as secure signature creation device for the electronic signature

The concept of a Smart Card Community is supported : all smart cards issued and managed by a given card issuer Card (Issuer Centric model) where the issuer is either a Government institute or acting under the responsibility of such a Government institute

The concept of cross schemes E-service communities is supported: all smart cards where the eAuthentication and signing capabilities are recognized by a given service provider



# Basic Functionalities

- electronic identification of the cardholder to public and private on-line services
- qualified electronic signatures for legal proof of non repudiation
- optionally support of confidentiality services, enabling encryption of data transmitted over a network
- optionally qualify as an official travel document (within the EU)



# Overall system requirements

- Issued in a face to face issuance process after establishing identity on the basis of reliable data (RA functionality)
- IAS applet to be detected automatically at start-up (ISO OID / Card Capabilities Discovery mechanism)
- Support of different classes of authentication/security environment, including a 'qualified' level
- mutual device authentication between a card and the card reading infrastructure shall be supported
- Minimum capacity and performance requirements for IAS execution, [t.b.c](#)
- Comply with some common elements in personalisation procedure, [t.b.d](#)
- Post issuance application downloading to be supported as an option
- Multi-vendor support (main issue: key management)
- Highly tamper & counterfeit resistant (EAL 4+ level)
- Support of Auditability (logging, card management info etc.)
- In compliance with international standards (ISO 7816 1-12, ISO 14443 1-3, JavaCard/GP (support of native & Java cards)
- Target life span for the card (physical & electronical) of minimal 5 years shall be guaranteed
- Lay out of the visual area's and data on the card are out of scope for WS eAut, in scope for CEN 224-WG 15



# User identification requirements

- Personal cardholder data shall be held on board the card in electronic form
- Personal data set shall contain as a minimum for interoperability the following data:
  - national identifier
  - family name, given name
  - sex
  - date of birth
  - place of birth
- Content and format of these data shall be based upon the ICAO Logical Data Set model

# User authentication requirements

PIN is required (ISO standard to be referred, PKCS #15 related)

Biometrics are optional

**If** biometrics are included the following applies:

- Biometric Pin for 1:1 verification
- a Biometric OID in support of multiple biometric technologies must be present
- Fingerprint minutia must be present (interoperability reasons)
- Image extraction on board the card is recommended
- Biometric template storage must be on board card the card
- Biometric matching on board the card for 1:1 verification is recommended
- Biometrics for 1: n is out of scope

Signature key for authentication purposes

- shall be present
- shall occur only once and cannot be derived
- shall be protected against unauthorized usage by PIN and/or Biometrics



# Electronic signature requirements

PKI shall be in compliance with the

- qualified digital signature as per article 5.1 of the EU directive 1999/93/EC on a Community framework for electronic signatures

PKI shall be in compliance with ETSI QCP 101456.

Main elements:

- registration procedures
- information content of a certificate
- liability of the certificate authority
- responsibility for protecting the eID card and its content
- loading of other applications on the card
- renewal of an eID card
- prevention of use of eID card and its certificates
- cancellation of an eID card
- requirements for the supporting PKI (i.e. CWA 14171)
- obtaining and protecting the CA certificate
- obtaining certificate status information



# Electronic signature requirements (cont.)

PKI shall be in compliance with CWA 14890 (area K) part 1 and 2:

- key pair generation on board card
- storage of keys on board card
- in compliance with 7816/15 (PKCS 15) and Crypto Objects
- signing function will be PIN and/or Bio protected
- data to be signed cannot be altered
- the format for electronic signatures and their certificates shall be interoperable
- secure messaging shall be supported (symmetric crypto)
- algorithms as in EU WS eSign algo document shall be supported
- public available certificate status verifying function for relying parties

PKI shall be implemented in the following way:

- minimum of 2 certificates (signing; auth and other functions/encrypt)
- certificates (X509V3) will hold as a minimum:  
name of CA, name Cert holder, unique identifier of Card Holder /Certholder, period of validity of certificate, serial number of certificate, info on certificate policy, purpose of certificate, liabilities



# More information/want to join in ?

- ***WS eAuthentication, July 6, Sept 20***
- ***CEN 224- WG 15 ECC***
- ***Next OSC Conference December 9-10 in Prague***
- ***<http://eeurope-smartcards.org>***
- ***[arkel@cardlife.nl](mailto:arkel@cardlife.nl)***